COLLUSION-RESISTANT SYBIL ATTACK DETECTION IN MOBILE AD HOC NETWORKS

By

Muhammad Sajid Khan
MSIS 09

Thesis submitted to the faculty of Information Security Department, College of Telecommunications (MCS), National University of Sciences and Technology, Pakistan in partial fulfillment for the requirements of MS in Information Security.

June, 2014

CERTIFICATE

It is to certify that final copy of Thesis has been evaluated by me, found specified format and error free.

Dated: ______ 2014

____
(**Lt Col Dr. Adnan Rashdi**)

ABSTRACT

A Mobile Ad-Hoc Networks (MANETs) is an autonomous collection of mobile devices that communicate over relatively bandwidth contrived wireless links. They are mainly convenient and appropriate for critical situations , including armed forces , law enforcement as well as emergency preparedness class of operations and catastrophic conditions to replace the damaged infrastructure networks.

Initially MANETs were commenced as supervised networks normally having ownership by a sole unit called offline authority, like military. Due to the increase in the mobile communication devices, an entirely self-organized and managed MANET may be produced. Because of openness, MANETs are subject to various adversarial attacks. In entirely self-organized MANETs, nodes are normally hesitant to expend their valuable resources forwarding the packets of other nodes and are therefore liable to evince selfish or occasionally spiteful malicious behavior. This selfishness can deprive network throughput and possibly lead to network segregation. Cooperation enforcement schemes have been proposed to thwart the issue of selfishness primarily to make sure selfish nodes bear the punishment of their bad actions. However, Due to the lack of centralized identity management or centralized Trusted Third Parties in MANETs, nodes can create zero-cost identities without any restrictions and could escape from punishment or detection by simply changing identity to clear all its bad history, known as whitewashing. Spiteful malicious nodes can concurrently create and command many virtual identities to launch an attack, called a Sybil attack. In Sybil attack, a large number of logical identities can be created on a single physical device by a selfish malicious node which gives a false impression to the network that it were different benign nodes and uses them to launch a harmonized attack against the network or a node. In the context of reputation-based schemes, a Sybil attacker can disrupt the detection precision by slandering other good nodes, boosting its own reputation or exchanging fake positive recommendations about one of its quarantined identities.

In order to defend against Sybil attacks, Position verification or localization of nodes seems most promising. Localizing a node requires cooperation of other nodes. But, nodes may not always behave cooperatively and may collude in unfriendly environments.

Collusion attacks in location verification engage multiple opponents conspiring to cheat the verifiers of the system into believing that there is a node at the specified location. Collusion attack normally takes place when two or more malicious nodes harmonized their potencies to save one or more Sybil nodes, launch a harmonized attack or to disrupt the detection precision. For example, some malicious colluding nodes may support and share positive recommendations for the Sybil identities of other spiteful nodes being evaluated, making it almost impractical to spot such identities as being Sybil.

A successful collusion attack often works on the principle that nodes shows itself as reliable and trustworthy and cooperate in some type of interactions, usually direct interaction and then deceive the node in witness interaction, i.e. providing false information about other nodes to support colluding group or defame or degrade other benign nodes. This forged information promotes the colluding group and the victims will interact with it and will be betrayed.

In this research project we figure out that if the assessor node employs a multi-dimensional trust model, collusion attack can be averted, i.e. Trust in Direct interaction as well as in witness interactions. The motivation for having two types of trust is that we believe trustworthiness has different independent dimensions. For example, a node that is honest in a direct interaction is not certainly trustworthy in a witness interaction. The sole purpose of indirect trust computation is to determine the trustworthiness of a (unfamiliar) node from the set of recommendations to slight the gap between the acquired recommendation and the real trustworthiness of the target node for detecting collusion. The proposed scheme is designed to compute the trustworthiness of every node, examine the activity pattern of nodes, detect, and thwart collusion and Sybil attacks.

A novel and robust trust based Sybil attack detection-resistant to collusion approach is proposed to accurately detect whitewashing and Sybil attacks in the presence of malicious collusion. We will show that detecting Sybil identities in the presence of collusion attack while exhibiting one-dimensional trust model cannot accurately detect Sybil identities. Through the help of extensive simulations and experiments, we are able to demonstrate that our proposed solution detects Sybil or whitewashers’ new identities with good accuracy and reduces the benefits of collusion even in the presence of mobility.

DEDICATION

All praise and thanks to almighty Allah, the most gracious and the most merciful, Master of the Day of Judgment. Guide us with courage and right path, path of those to whom you have bestowed your blessings.

Dedicated to my beloved parents and wife, brothers and my lovely Sister for their love, endless support and encouragement

ACKNOWLEDGEMENTS

First and foremost I must thank ALLAH, The Most Beneficent and The Most Merciful, for giving me the ability, strength and determination to do the MS at this prestigious institution.

Then, I duly acknowledge consummate supervision of my supervisor Lt. Col. Dr. Adnan Rashdi, who inculcate the importance of research phase and taught me about carrying out quantitative and qualitative research. I want to show my cordial gratitude to my committee members, Lt. Col. Arif Wahla, Dr. Naima Iltaf and Lecturer Waseem Iqbal for their kind support and guidance.

I am very thankful to my parents and other family members for their prayers and support which enabled me to successfully complete my MS.

Special thanks go to Dr. Naima Iltaf of the Military College of Signals, National University of Sciences & Technology for her mentorship and assistance. Her constant motivation and guidance enabled me to think and write more clearly and to face audaciously the hurdles during my research.

I am also deeply obliged to Dr. Sohail Abbas of University of Malakand for his precious time that he dedicated to my research work and discussion on ideas that eventually helped solidify many of the new concepts presented in this thesis.

TABLE OF CONTENTS

LIST OF FIGURES

Figure Number ***Page***

LIST OF TABLES

Table Number ***Page***

Chapter 1

INTRODUCTION

1.1 Overview

Recent advances in computer networking have introduced a new technology for future wireless communication, known as mobile ad hoc network (MANET). A MANET is an autonomous collection of mobile devices that communicate over relatively bandwidth constrained wireless links. Nodes can join or leave the network at any time and they can freely roam across the network.

MANETs were originally introduced as closed or managed networks that belonged to a single entity called an offline authority, such as the military. As belong to a single offline authority, all nodes are motivated to cooperate to achieve a common goal. Due to the increase in the mobile communication devices like PDAs, cell phones, laptops and other intelligent radio devices, a *fully* self-organized mobile ad hoc network may be produced.

Besides other security issues, one of the serious issues is the Sybil attack [3]. In Sybil attack, a malicious node can generate and control a large number of logical identities on a single physical device which gives the illusion to the network as if it were different legitimate nodes and uses them to launch a coordinated assault against the network or a node. Sybil attacks can disrupt important protocols, such as Distributed Storage, Routing, Data Aggregation, Voting, Misbehavior Detection, and Traffic Congestion in a Vehicular Ad hoc Network (VANET) [12].

In order to defend against Sybil attacks in wireless sensor networks, Perrig et al. [6] proposed three types of techniques that are radio resource testing, registration and position verification. Position verification (which is usually based on signal strength) seems most promising among the three because it is lightweight and even can be used without the use of GPS. This cannot only detect Sybil attacks, but also prevent other attacks such as masquerading and man-in-the-middle attacks [8].

By surveying Signal strength based location systems for wireless networks we have found that node cooperation is very important for detection of Sybil attack, but in civilian ad hoc networks, nodes often belong to different individuals and have their own interests. Consequently, nodes may not always behave cooperatively and may collude in such environments. Moreover, nodes can also be captured and tampered with by the enemy in the hostile environment in order to disseminate false information for disrupting the detection accuracy of such systems.

Inaccurate witnesses and the existence of cheaters cannot be ignored in ad hoc networks. In a witness-based collusion attack, an unreliable witness provider - in spite of being cooperative in its direct interactions provides high ratings for other malicious nodes (other members of the colluding group), thus resulting in motivating the victim node to interact with them. This inaccurate information can challenge the integrity of the detection system, mostly based on witness information leading to misleading trust information and possibility of collusive behavior to promote or sideline a user or group of users. Collusion occurs when two or more malicious nodes coordinate their efforts to protect one or more Sybil identities or to disrupt the detection accuracy. For instance, some malicious nodes may vouch for the Sybil identities of other malicious nodes being tested, making it impossible to identify such identities as being Sybil.

This research work is based on Sybil attack detection in Mobil ad hoc networks by analyzing RSSI of each new node or ID in the network, specifically in the presence of malicious colluding nodes or more specifically collusion attack which can disrupt the detection accuracy of Sybil nodes. The focus remains on the revealing of malicious or selfish colluding nodes while detecting Sybil nodes with special attention to incorporating trust based mechanism that would mitigate the benefit (the payoff gained from collusion) transfer among nodes. This notion of trust will act as an incentive for nodes which will motivate nodes to cooperate. In the end, overall organization of this thesis is described.

1.2 Related Work

In Sybil attack, a malicious node can generate and control a large number of logical identities (impersonates other nodes by broadcasting messages with multiple node identifiers (ID)) on a single physical device which gives the illusion to the network as if it were different legitimate nodes and uses them to launch a coordinated assault against the network or a node. In order to defend against Sybil attacks in wireless sensor networks, Perrig et al. [6] proposed three types of techniques that are radio resource testing, registration and position verification. Position verification (which is usually based on signal strength) seems most promising among the three because it is lightweight and even can be used without the use of GPS. This cannot only detect Sybil attacks, but also prevent other attacks such as masquerading and man-in-the-middle attacks [8]. Existing solutions for Sybil attack prevention are too costly for the resource-poor mobile and sensor platforms. A received signal strength indicator (RSSI) based solution (a type of position verification) for Sybil attack is desirable as it does not burden the WSN with shared keys or require piggy backing of keys to messages. Ideally, upon receiving a message, the receiver will associate the RSSI of the message with the sender-id included in the message, i.e. bound to a single physical node and must move together, and later when another message with same RSSI but with different sender-id is received, the receiver would complain of a Sybil attack.

Zhong et al. [16] showed that no sensor node can hide its location in an environment where it is monitored by four or more nodes for detection of Sybil attack. Demirbas et al. [17] implemented Zhong‘s algorithm of localization by conducting a large indoor experiment of static MICA 2 motes. Niraj et. al [10] proposed a robust distributed malicious node detection and precise localization and tracking method for Cluster based MANET and detection Sybil nodes. Mourad et. al in [11] proposed an original decentralized dynamic method for localization based on intervals for Sybil attack detection. Jiangtao et al. [18] proposed a Sybil node detection scheme for static clustered wireless sensor networks using RSSI and status information aggregated in the head nodes. Shaohe et al. [19] proposed a Cooperative RSSI-based Sybil Detection (CRSD) scheme for static sensor networks where all nodes, intimate or malicious, should have fixed transmission power. Hao et al. [25] proposed a security protocol to detect Sybil attacks for position based applications in privacy preserved vehicular ad hoc networks

(VANETs). But for all the above schemes, node cooperation is very important for detection of Sybil attack, but in civilian ad hoc networks, nodes often belong to different individuals and have their own interests. Consequently, nodes may not always behave cooperatively nor they trust each other and may collude in such environments. Moreover, nodes can also be captured and tampered with by the enemy in the hostile environment in order to disseminate false recommendations for disrupting the detection accuracy of such systems.

Collusion attacks occur when one or more users conspire together to take advantage of breaches in trust models to defraud one or more users. It can be the case that users in the colluding group adopt a sacrificial stance in collusion attacks in order to maximize the utility of the colluding group.

All the above schemes use cooperation for their detection of Sybil nodes however; nodes can share false recommendations while colluding with other nodes or their own virtual identities to disrupt the detection accuracy.

This research work is focused on detection of Sybil attack in MANETs in the presence of malicious collusion; and also detecting and excluding malicious colluding nodes.

1.3 Problem Statement

Node cooperation is very important for detection of Sybil attack in RSSI Based detection schemes. In civilian ad hoc networks, nodes often belong to different individuals and have their own interests. Consequently, nodes may not always behave cooperatively and may collude in such environments. Moreover, nodes can also be captured and tampered with by the enemy in the hostile environment in order to disseminate false information for disrupting the detection accuracy of such systems.

Inaccurate witnesses and the existence of cheaters (exploitation) in artificial societies, i.e., Networks employing trust and reputation models, cannot be ignored. In a witness-based collusion attack, an unreliable witness provider - in spite of being cooperative in its direct interactions provides high ratings for other malicious nodes (other members of the colluding group), thus resulting in motivating the victim node to interact with them. This inaccurate information can challenge the integrity of the detection system, mostly based on witness information leading to misleading trust information and possibility of collusive behavior to promote or sideline a user or group of users. Collusion attacks in location verification involve multiple adversaries cooperating to cheat the verifiers of the system into believing that there is a node at the claimed location. Collusion occurs when two or more malicious nodes coordinate their efforts to protect one or more Sybil identities or to disrupt the detection accuracy. For instance, some malicious nodes may vouch for the Sybil identities of other malicious nodes being tested, making it impossible to identify such identities as being Sybil.

Based on our study, if the assessor node employs a multi-dimensional trust model, collusion attack in Sybil nodes detection can be averted.

1.4 Thesis Objectives

An objective of this thesis is to develop a novel and robust trust based Sybil attack detection scheme resistant to collusion; which accurately detect whitewashing and Sybil attacks in the presence of colluding nodes. More specifically the scheme should have the following capabilities: It should have a reasonable tolerance against collusion. The collusion resistance may be achieved by incorporating trust based mechanism that would mitigate the benefit (the payoff gained from collusion) transfer among nodes. This notion of trust will act as an incentive for nodes which will motivate nodes to cooperate. The scheme should have secure information dissemination mechanism such that a bad node cannot defame or spread rumor about good nodes. We will show that detecting Sybil identities in the presence of collusion attack while exhibiting one-dimensional trust model cannot accurately detect Sybil identities. Through the help of extensive simulations and experiments, we will demonstrate that our proposed solution detects Sybil or whitewashers’ new identities with good accuracy and reduces the benefits of collusion even in the presence of mobility.

1.5 Thesis Outline

The thesis consists of six chapters. Chapter 1 presents a brief introduction to the problem in hand. Chapter 2 presents a brief introduction to Mobile ad-hoc Networks and security issues in MANETs, such as Sybil attack and Collusion attacks. Chapter 3 provides a detail description of localization and RSSI based Sybil attack detection schemes in MANETs. This chapter encompasses preliminary information about why traditional RSSI based schemes are not appropriate for detection of Sybil attacks accurately in the presence of colluding nodes and reflects the requirement of a multi-dimensional trust model for detecting and preventing collusion attacks in MANETs. Chapter 4 explains the proposed approach for Collusion resistant Sybil attack detection in MANETs, in detail. Chapter 5 discusses the implementation and then performance analysis of the proposed scheme. Analyzes and compares the security and efficiency of the proposed scheme with the existing Sybil attack detection schemes. Finally, chapter 6 concludes the whole thesis and gives direction for future work.

Chapter 2

MOBILE AD-HOC NETWORK (MANET) SECURITY

2.1 Introduction to MANETs

MANET is an acronym for Mobile Ad-hoc Network. It is collection of multiple nodes that formulates; either, a temporary or permanent, self-organized wireless network that don't rely on any pivotal central architecture or control. As depicted in Figure, the nodes can be either any laptops, hand held portable devices like mobile phones etc. In MANET, all subsidiary nodes are free to join or leave the network at any instant. Moreover, nodes are also free to roam in the network freely. MANETs are autonomous to determine its basics configurationally requisite parameters; like addressing and routing. Nodes can also act as a host as well as a router, thus relaying data to extend the range of nodes that don't fall in the mutual direst range. MANETs are class of mobile networks, that has been specially designed to use in situations where there infrastructure is either non-existent or it's extremely costly to deploy basic infrastructure. Such scenarios include, disaster relief operations where the core infrastructures has collapsed, search and rescue operations over a wider area, casual meeting, robot networks etc.

An overview of the MANET and its Security requirements are presented. In the end, a detailed analysis of Sybil and Collusion attacks are presented. An analysis is made for a feasible trust model for 'Collusion-resistant Sybil attack detection in MANETs is made to meet the security requirements of future networks.

Figure 2.1: Mobile ad hoc network (MANET)

2.2 Brief Review of Network Security

In these sections, basic security devices pertaining to the network security has been presented based on the literature review [32, 33, 34].

2.2.1 Confidentiality is one of the basic primitives of security and it is aimed at provisioning and preserving secrecy of a message over an even an insecure medium. Thus, content of the original message remain confidential between the sender and receiver and are not disclosed to unintended recipients and other parties. In case of MANETs, confidentiality is pretty tough to maintain mainly due to the broadcast nature of the wireless nodes and obvious nature/threat of eavesdropping associated with it. Due to this peculiarity, various security mechanisms and techniques, like secure key distribution mechanism are more difficult.

2.2.2 Authentication verifies the identities of sending and receiving parties in a network. One of the important attack against authentications attribute is masquerading attack. Whereby, an attacker pretends to be a legitimate user. It is very difficult detect these types of attackers in MANETs because due their inherent nature, there is no central authority to control certificates and key distribution to ensure identity authentication.

2.2.3 Integrity ensures that contents of message, while in transit, should not be modified in any sense by the unauthorized parties. Precisely, integrity safeguards unauthorized modification of message for example addition, deletion, introduction of unnecessary delays etc.

2.2.4 Access Control tightly controls access of only legitimate users to resources. It ensures that services, resources or data are accessed by the users according to their access rights and privileges. To breach access control mechanism, an attacker can use numerous techniques including masquerading, message fabrication, interception and modification.

2.2.5 Availability is an important attribute of information security. It ensures that services or devices are always available to the legitimate intended users. In case of MANETs, one of the potential issues is that nodes in the network are usually resource constrained having very low powered devices. So an attacker can simply engage these devices to exhaust their battery, thus hindering availability to the users.

2.2.6 Non-Repudiation is an important feature and it ensures that sender or a receiver of a message shouldn't be able to deny the sending or reception of a message. Attack on non-repudiation can be masquerading.

2.3 MANETs Security Implications

D. Djenouri et al. [32]. Srivatsa [4] highlighted various security concerns of MANETs. These includes few similar to the wired networks, some are due to the very nature of wireless connectivity, while others are new. First and foremost, since the wireless network broadcast many attributes in the network, therefore, an attacker can very easily eavesdrop on data and/or inject bogus data into the network. Secondly, network devices in these wireless networks are extremely resource constrained; having low power, computational capability, memory and bandwidth, so all of these can be exploited by the adversaries. Thirdly, due non availability of any centralized Trusted Third Party (TTP) in a mobile ad hoc network poses new challenges for robust and efficient trust and identity management. Fourthly, nodes in ad hoc networks are presumed to be cooperative in nature thus facilitating mutual relay of packets; however, any selfish, compromised or malicious node may violate this trust assumption thus posing security threats. Fifthly, nodes in wireless networks are mostly portable handheld devices, therefore, these are more vulnerable to physical security threats their counterparts in wired networks.

Due peculiar nature of MANETs, having lack of concrete infrastructure, continuously changing network topology due nodes mobility, security implications becomes much challenging. Usually, nodes are small hand-held devices, including PDAs, smart phones and palmtops; therefore, their physical security can be very easily compromised. The situation may become very precarious when an adversary manages to exploits numerous nodes, consequently, launches an insider attack in a sensitive network, like any military network. Due to the aforementioned constraints, the security protocols presently employed or proposed in existing wired networks may not be equally effective in MANETs. Therefore, there is a dire need that MANET security protocols must be able to scale instantly to meet network demands, while on the other hand their performance should not be affected due dynamic network topology.

Idea of MANETs was originally conceived as closed or managed networks that belonged to a single entity/organization known as an offline authority, like the military. In such typical scenarios, end users have a pre-established and pre-configured relationship. Moreover, the nodes work under this offline authority. Nonetheless, with the advent and recent boost in use of mobile communication devices such as laptops, PDAs, cell phones etc in self-organized mobile ad hoc network, nodes do not belong to any particular single entity or organization. All end-users or nodes formulate a network in a purely ad hoc manner. Therefore, due non-existent TTP and presence of numerous un-trusted users in a fully self-organized MANET, under mentioned security problems caused, as presented by Mcdonald et al. [2].

- Fully self organized MANETs are quite open in nature. Nodes are likely to join and leave the network at random, just like internet. This openness attributes largely attracts malicious and selfish users.
- At each end, network user will be its own authority in the domain, therefore, solely responsible to accomplish requisite distributed network functionalities independently; like, packet forwarding for other nodes in the network, generating own key etc.
- Threat perception from active insider attacks in the network always persists.
- As Douceur [3] highlighted that, due absence of an offline TTP, any node in mobile ad hoc network can create and control more than one identity without any additional cost or difficulty. This is termed as a Sybil attack. Consequently, single node can join the network under a different identity, therefore, it becomes very difficult to track and subsequently hold malicious nodes accountable for their deeds.

Routing in MANETs is based on multihoping, i.e. for communication range extension of single node, each node forwards other adjacent nodes' packets. Nevertheless, in case of open MANETs, nodes might not cooperate with each other thus exhibiting selfish behavior including not forwarding packets and collaborating with other malicious nodes to disrupt the essential network services. Ultimately, this selfish attitude of nodes results in degradation of overall network performance.

2.4 Cooperation in Self-Organized MANETs

Self-organized systems have gained tremendous boosts and resultantly widespread attention in terms of research and deployment, especially in the last decade. These types of systems are organized in accordance with the principle of Peer-to-Peer (P2P) organization; whereby, each participant in the system have level playing field in terms of responsibilities and capabilities, i.e. all nodes are peers in the network system.

There are numerous routing protocols exclusively developed for MANETs. These include Dynamic Source Routing (DSR) [35], Destination-Sequenced Distance-Vector (DSDV) [37] and Ad hoc On-demand Distance Vector (AODV) [36] that are based on the multihop propagation assumption; that means, each node in the network must cooperate with others and forward other nodes’ data packets to achieve range extension and overall network performance enhancement. This multihop assumption is only valid for closed or managed MANETs where nodes only belong to a single entity or organization. However, in case of fully self-organized open MANET, this assumption might not hold good because all the nodes have their own domains and objectives. Since, nodes in MANETs are extremely resource constrained, therefore, each data packet transmission consumes certain amount of computational power. Therefore, nodes tend to preserve computational power and battery, thus obviously, nodes might be reluctant to spend their precious resources forwarding other nodes’ packets. Therefore, selfish or sometimes malicious behavior in open MANET environments is quite often expected. Selfish nodes are thoese nodes that utilize the services provided by other adjacent nodes but that do not contribute their own services to the network with the intention to save their own resources. This unwanted selfish behavior of certain nodes may lead to network partitioning and overall degradation in performance. It has been shown by Agrawal et al. [38], that even a small percentage of selfish nodes can significantly disrupt the entire network thus severely degrading the network performance.

In order to enforce mutual cooperation and discourage selfish behavior among nodes in MANET, three major schemes have been proposed in the literature. These include a) Reputation based, b) Trust based and c) Credit based models. Reputation and trust based schemes utilizes the past behavior of node to predict and to decide about the trustworthiness and cooperation of other nodes. Consequently, nodes that have high reputation or trust index are provided with the services, while others with low reputation or trust are eventually isolated from the network. Nodes usually pay for services in credit-based schemes. Virtual currency mechanism is enforced for payments in these models. Nodes can be either buyers and/or sellers of the packet forwarding services. Nodes must possess credit to forward their packets in the network.

Major drawback with credit-based models is that these are not scalable because they need a centralized virtual bank to regulate the transactions mechanism. Additionally, for enhancing security, each node is also equipped with tamper proof hardware. Due to aforementioned reasons, credit-based schemes are considered not viable for MANETs application. Whereas, reputation or trust-based models do not require any centralized mechanism or tamper proof hardware, therefore, they can be implemented in a fully distributed manner to increase scalability, hence are considered viable for use in MANETs. Since our focus in this research is on reputation-based schemes only, therefore, we will not discuss credit-based schemes further. Nonetheless, details for credit base schemes have been presented by Agrawal et al. [39] and Mandalas et al. [40].

2.5 MANETs and Sybil Attacks

Usually, communications in wireless networks are based on a unique identity that indicates a particular network entity: a node. Identity of each node is an address to communicate with a network entity. Resultantly, a one-to-one mapping is formed between an identity and an entity. Moreover, it is usually assumed that either implicitly or explicitly by many mechanisms; therefore, two unique identities correspond to two distinct nodes [19]. Malicious nodes can exploit it and illegitimately claim multiple identities, thus, violating one-to-one mapping of identity and entity. This has been termed by Douceur [3] as a Sybil attack, where an attacker or a malicious node is able to both generate and control a large bunch of logical identities on a single physical device. It gives the delusion to the network as if there are different legitimate nodes. These are then used to launch a coordinated assault against either the network or a node.

It is important to note that in case of trust and reputation-based models, any Sybil attacker can also disrupt the detection accuracy by defaming other good nodes. It can also either self-promote itself or exchanging false positive recommendations about one of its quarantined identities. In the literature, Perrig et al. [6] has identified the various security protocols of ad hoc networks that can be affected by Sybil attacks. These include Distributed Storage, Data Aggregation, Routing, Misbehavior Detection, Voting, and Traffic Congestion in a Vehicular Ad hoc Network (VANET) [12].

Defending wireless sensor networks against Sybil attacks, Perrig et al. [6] proposed three types of techniques; radio resource testing, position verification and registration. Among these, radio resource testing technique is based on unrealistic assumptions that a radio must send and receive on a single channel simultaneously. However, multiple radios with multiple channels are common foe wireless network and is in vogue in wireless mesh networks. On the other hand, registration technique requires trusted third party involvement for identity issuance, verification and revocation. This altogether doesn’t suit the ad hoc network architecture. Position verification is another proposed technique that is mainly based on signal strength. It seems most promising among the three because of certain advantages associated with it; lightweight scheme and it can also be used without the use of GPS. In case of position verification technique, each network nodes verify the position of each other node. It also ensures that each physical location is bounded by only one identity at any particular time instant. Therefore, position verification can’t only detect Sybil attacks, but it can also prevent other attacks like masquerading and Man-In-The-Middle (MITM) attacks [8].

Position verification systems or location system can be further sub divided into three distinct sub-components. These are, distance/angle estimation, position computation and Localization algorithm. Location system can be greatly affected by any small misbehavior in any of these components. For example, malicious erroneous distance estimation can result in a position miscomputation that will subsequently be propagated to the localization algorithm and consequently may cause a major localization error for the sensor nodes. Therefore, efficiency of location-based services depends solely on the truthfulness of the localization result.

Detailed survey of the signal strength based location systems for wireless networks reveals that mutual node cooperation is very important for detection of Sybil attack. However, main problem in node cooperation is that in practical civilian based ad hoc networks, contributory nodes usually belongs to different entities , thus have their own interest. As a result, nodes might not always co-operate and may collude in such environments. In addition, nodes can also be captured and tampered with by the adversary in the hostile environment for disseminating false location information thus resulting in disrupting the detection accuracy of location based systems.

This research work is based on Sybil attack detection in Mobil ad hoc networks by analyzing RSSI of each new node or ID in the network, specifically in the presence of malicious colluding nodes or more specifically collusion attack which can disrupt the detection accuracy of Sybil nodes.

2.6 Collusion Attacks in MANETs

In recently published literature, various researchers have also identified the existence of cheaters (exploitation) in artificial societies that employ trust and reputation models with the existence of inaccurate witnesses [41]. Inaccurate information of such type can challenge the integrity of the reputation system based on witness information, and ultimately may lead to misleading trust information. Moreover, there is also possibility of collusive behavior to promote or sideline a legitimate user or group of legitimate users. Salehi-Abari et al. in [26] also define collusion as “A collaborative activity that gives to members of a colluding group benefits they would not be able to gain as individuals”.

When one or more nodes conspire together to take undue advantage of breaches in trust models to defraud one or more nodes, the collusion attacks occur. Nodes in the colluding group may adopt a sacrificial stance in collusion attacks in order to maximize the utility of the colluding group. Usually, collusion attacks work based on the core idea that one or more nodes show themselves as trustworthy nodes in one type of interaction (usually direct interaction). Later on, they will be untrustworthy in other type of interactions (e.g., witness interaction) by providing misinformation in respect of other members of the colluding group. This false information might encourage a victim to interact with members of the colluding group. Consequently, if victim interacts with them, the members of the colluding group will cheat the victim.

As shown in Figure, three roles are defined in case of the Witness-based Collusion Attack. These include; victim/ Evaluator node, malicious node and enticer/ witness node. Among these three, enticer nodes and malicious nodes formulate the colluding group to exploit victim nodes. The enticer/ witness nodes exhibits trustworthy behavior in direct connections to victim node and resultantly they also become trustworthy neighbors of victim nodes. Subsequently, when victim nodes tends to look for ratings (reputation) of malicious node by asking their trustworthy neighbors, then the enticer nodes, being the neighbors, provide high ratings for malicious nodes (other members of the colluding group) thus encouraging victim nodes to interact with them. Ultimately, victim nodes will be exploited by them. The Fig below, the dashed line depicts start of interaction of a victim node with a malicious node as an outcome of high ratings provided by enticer nodes.

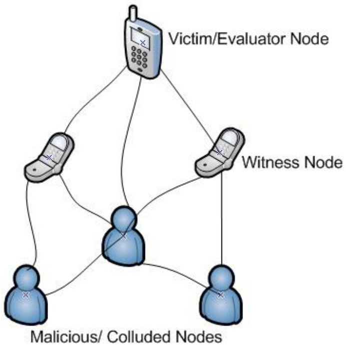


Figure 2.2: Witness based Collusion attack

From Fig above, it can be deduced that that when the victim node basis its assessment of witness information on the cooperation (trustworthiness) in direct interactions, this attack will be successful. Specifically, the success of this attack is the outcome of the inappropriate assumption that whoever node is cooperative (trustworthy) in direct interactions will also be cooperative (trustworthy) in providing witness information regarding other nodes. There are two forms of collusion attacks on witness based trust management. Detail of the same is covered in ensuing paragraphs:

2.6.1 Target—witness interaction

This behavior of colluding users applies to a node requesting trust values for a target through a witness. Figure shows an example of node A (evaluator) requesting trust values for node E (target). Only intermediate nodes C and D have direct interaction with both evaluator A and the target E and therefore posses a trust value. Both C and D can pass on the trust recommendations for E, to the evaluator A. B can also provide a trust rating for E, but since it doesn't interact directly with E, it has to rely on witness recommendations from F, therefore a direct referral from C or D would be preferable. C can collude with malicious target E to provide false positive recommendations to the evaluator subsequently promoting target E as a trustable user.

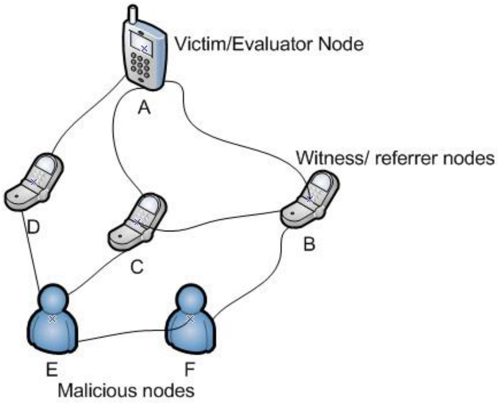


Figure 2.3: Target-Witness Collusion attack

2.6.2 Witness—witness interaction

A group of malicious nodes can collaborate to recommend false trust values for a member of group to gain access to resources. In case when an evaluator node cannot find direct recommendations from immediate neighbors it relies on recommendations from witnesses. Figure 1b shows collusive behavior among witnesses. The evaluator A, obtains recommendations for target H. As before A has no prior knowledge of trust values for H.

B, C and D can all provide independent trust values to A, honestly, based on recommendations from nodes E and F. It can be seen that both witness providing nodes can collude to provide false values to promote H or to present H as an untrustworthy user. Figure 1b shows collusive behavior among malicious nodes collaborating to pass false information to B, C and D, thus affecting trust values for evaluator A.

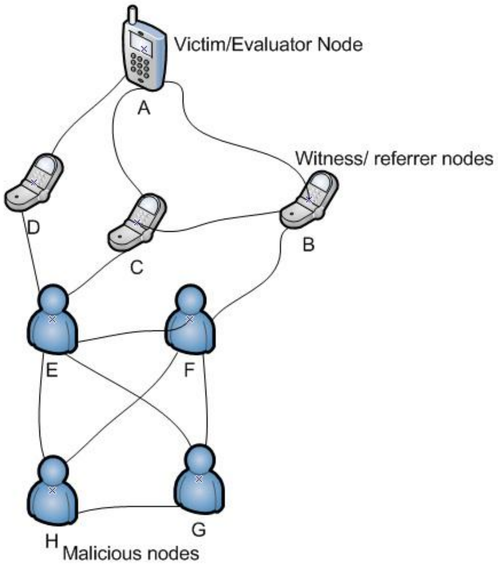


Figure 2.4: Witness-Witness Collusion attack

Based on abovementioned cases, it can be deduced that when the victim/evaluator node basis its assessment of witness information on the co-operations (trustworthiness) in direct interactions, the collusion attack is very likely to be successful. Specifically, the success of this attack is the consequence of assumption that whoever is cooperative (trustworthy) in direct interactions will also be cooperative (trustworthy) in providing witness information regarding other nodes.

The hypothesis of this research is that the Witness-based Collusion Attack can be prevented if the asker node utilizes an independent multi-dimensional trust model. Precisely, the asker node will assess the witness providers based on their cooperation in witness interactions.

To the best of our knowledge, there is no formal model of accurately detecting Sybil attacks in the presence of malicious collusion and detecting and excluding those colluding nodes, analysis of the level of encounter risk of malicious collusion on the detection accuracy of Sybil attacks in MANETs. A successful collusion attack often works on the principle that nodes shows itself as reliable and trustworthy and cooperate in some type of interactions, usually direct interaction and then deceive the node in witness interaction, i.e. providing false information about other nodes to support colluding group or defame or degrade other benign nodes. This forged information promotes the colluding group and the victims will interact with it and will be betrayed. This lack of study on witness-based collusion attacks while cooperative detection of Sybil attacks motivates the work reported in this paper.

This research work is focused on Sybil attack detection in MANETs, specifically in the presence of collusion attack. The focus remains on the revealing of malicious or selfish colluding nodes while detecting Sybil nodes with special attention to incorporating trust based mechanism that would mitigate the benefit (the payoff gained from collusion) transfer among nodes. This notion of trust will act as an incentive for nodes which will motivate nodes to cooperate. Our contributions include the introduction of witness-based collusion attacks in the detection of Sybil attacks in MANETs; an analysis of the impact of malicious collusion on Sybil attack detection in MANETs; and development of a novel and robust trust based Sybil attack detection scheme resistant to collusion and incorporating trust based mechanism that would mitigate the benefit (the payoff) gained from collusion.

2.7 Conclusion

We reviewed several key concepts important to this thesis in this chapter. The reviewed topics include network security, mobile ad hoc networks and – and the threats that seriously endanger the mobile ad hoc networks. We also discussed the issue of Sybil attacks and effects of malicious collusion in detection of Sybil attacks. It has been showed that when a node bases its assessment of witness information on the inappropriate assumption that whoever is trustworthy in direct interactions will be trustworthy in providing witness information regarding other nodes is the basis of success of collusion attack and will eventually inaccurately detect Sybil nodes. This reflects the requirement of a multi-dimensional trust model for detecting and preventing collusion attacks in MANETs.

Chapter 3

SYBIL ATTACK DETECTION AND COLLUSION

3.1 Introduction

A large number of logical identities can be generated and also can be controlled by a malicious node when performing a Sybil attack using a single device and that may give illusion to that network as if it was originated from the legitimate node and will use it so that it can launch an assault based on the coordination to either network or node. This attach occurs in the distributed environment. Each of the nodes gets awareness of the other node with the help of communication channel messages. This attacker i.e. Sybil attacker send different identifiers so that it can assume different identity. Each node join network each time with different identities, in the absence of TTP, holding malicious nodes is difficult that is accountable for such kind of actions. Sybil attacks disrupt certain kind of important protocols, such as Distributed Storage, Routing, Data Aggregation, Voting, Misbehavior Detection, and Traffic Congestion in a Vehicular Ad hoc Network (VANET) [12]. When using multiple identities to broadcast a message, a Sybil node may be rigging the vote on group-based decisions and can disrupt network middleware services severely.

Perrig et al. [15] proposed techniques of three different types that are radio resource testing, registration and position verification so that to defend against Sybil attack.

Radio resource testing is a technique is based on unrealistic assumptions that single channel is used for both sending and receiving. Wireless mesh topology usually use in multiple radio multiple channel. A trusted third party will be required for registration of identity issuance, verification and revocation that is not suitable for the ad hoc network. Even then an attacker retrieves information for which he is not authorized when using trusted third party. Position verification (based on signal strength) among the three is a lightweight and can be used without GPS. The position of each node and to ensure the physical location of each node is bounded by one identity at a particular time is verified by network node in the position verification. It not only detects Sybil attack but may also prevent certain other kind of attacks like for example masquerading and man-in-the-middle attacks [20].

The different number of solutions in order to prevent Sybil attacks is too much costly. A received signal strength indicator (RSSI) for Sybil attack which is a type of position verification solution is desirable because it won't burden the WSN with the pre-shared keys or it may require another technique called piggy backing to the keys. When a message is received, the RSSI of message will be associated by the receiver that will also include the sender-id in the message i.e. it will be bounded to a single physical node and movement will be all together, and whenever a receiver later receive a message with RSSI same and different sender ID, the receiver will complain that a Sybil attack has occurred.

This chapter concludes all schemes that cover detection of Sybil attack and some weaknesses in these schemes. This chapter concludes that all existing schemes for detection of Sybil attack in the presence of collusion fail to detect the attack effectively. The schemes presented till date between malicious nodes are also vulnerable to collusion. And because of these vulnerabilities the malicious nodes protects one or more than one Sybil identities. Some of the malicious nodes for instance may vouch for the Sybil identity of other nodes that are malicious in nature tested, will make it impossible to identify such kind of identities that are being Sybil in nature.

To the best of our knowledge, there is no formal model of accurately detecting Sybil attacks in the presence of malicious collusion and detecting and excluding those colluding nodes, analysis of the level of encounter risk of malicious collusion on the detection accuracy of Sybil attacks in MANETs. This lack of study on witness-based collusion attacks while cooperative detection of Sybil attacks motivates the work reported in this paper.

3.2 Existing Sybil Attack Detection Schemes

A malicious node in the Sybil attack may own several kinds of impersonated/fake identities and are presented in the network to the other nodes. It can reveal by a technique called position verification. Probability of Sybil attack becomes very high when different nodes are located at same position.

In recent years, many Sybil attack detection scheme have been proposed to detect Sybil nodes in wireless communication network [7] [11] [12] [17] [18] [19] [22]. All the schemes outlined here have assumed that there will be no collusion among malicious nodes and nodes would be trustable and cooperative.

As Position verification or localization of nodes seems most promising in detecting Sybil attacks, it requires cooperation of other nodes. But, nodes may not always behave cooperatively and may collude in unfriendly environments. Collusion attacks in location verification engage multiple opponents conspiring to cheat the verifiers of the system into believing that there is a node at the specified location. Collusion attack normally takes place when two or more malicious nodes harmonized their potencies to save one or more Sybil nodes, launch a harmonized attack or to disrupt the detection precision. For example, some malicious colluding nodes may support and share positive recommendations for the Sybil identities of other spiteful nodes being evaluated, making it almost impractical to spot such identities as being Sybil.

In the following sections, different existing Sybil attack detection schemes for wireless communication are discussed. All the schemes outlined here have assumed that there will be no collusion among malicious nodes. The weaknesses in these anonymous authentication schemes are also outlined.

3.3 Demirbas's Scheme

Demirbas's [17] proposed RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks. This scheme proposed a Sybil attack detection technique which is efficient, lightweight and GPS free. The technique is based on measuring the Signal Strength as described in [17]. Three cooperating nodes measure the Signal Strength when receive a message. After the obtained values are exchanged, calculate the ratio and store this sender record in the neighbor database. This ratio which is a unique ration mat determines the position of the node. This section will also outline some of the weaknesses in the scheme.

3.3.1 Review

Demirbas's assumed a static network, where all nodes are immobile after initial deployment. They assumed an initial set of nodes that are trustworthy (non-Sybil). Later on the new nodes are introduced as part of re-populating the network, some may behave like Sybil. The details are as under:

A. Localization with power

In [16] Demirbas' proposed RSSI based localization scheme. Demirbas's implemented Zhong's [16] schemes for the purpose of Sybil attack detection performing a number of schemes of static MICA 2 motes. If at least four sensors monitor radio signals, then none of the user will be able to hide itself. Suppose a node i may receive radio signal from node 0, then the RSSI will be as:

$$R_i = \frac{P_0.K}{d_i^{\alpha}}$$

P_0 is transmitter power, R_i represent RSSI, and K is a constant value, d_i is Euclidean distance, and α is distance-power gradient. Now let us suppose that a node j receives radio wave from node 0 at the same time, and then the P_j is similar to above equation.

The RSSI ratio of node i to j is:

$$R_i / R_j = (\frac{P_0.K}{d_i^{\alpha}}) / (\frac{P_0.K}{d_j^{\alpha}})$$

$$= (\frac{d_i}{d_j})^{\alpha}$$

User's location (x, y) can be computed by solving following equation through four receivers, i, j, k, and l:

$$
\begin{aligned}
(x-x_i)^2+(y-y_i)^2 &= (\frac{R_i}{R_j})^{\frac{1}{\alpha}}((x-x_j)^2+(y-y_j)^2) \\
&= (\frac{R_i}{R_j})^{\frac{1}{\alpha}}((x-x_k)^2+(y-y_k)^2) \\
&= (\frac{R_i}{R_j})^{\frac{1}{\alpha}}((x-x_l)^2+(y-y_l)^2)
\end{aligned}
$$

Where x_i and y_i is the location of node i, and other node.

B. Basic Algorithm RSSI-based Sybil Node Detection

Sybil attack detection is possible when using the localization algorithm in [16] Upon receiving a message, the four detector nodes compute the location of sender using equation 3 and associate this location with the sender-ID included in the message. Later when another message with different sender-ID is received and the location of the sender is computed to be the same as the previous one, the nodes detect a Sybil attack.

Let us consider four monitoring nodes have ID as D1, D2, D3, and D4 and an ID that is forged by a Sybil node as S1, S2, and so on with time as shown in Figure.

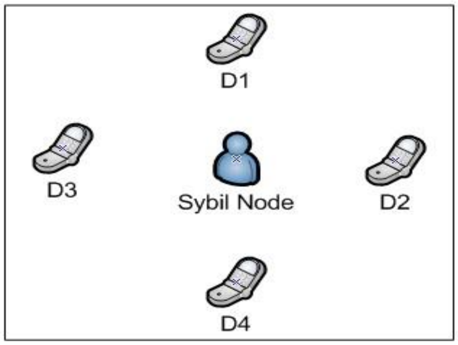


Figure 3.1: Location based Sybil attack Detection

At time t1, messages along with forged ID as S1 are broadcasted by a Sybil node. Monitoring four neighboring nodes receive the radio power and the forged ID. Each nodes transmits messages with its own ID and the received RSSI from Sybil node to representative node, D1. Note Rk i denotes the RSSI value when sender k receives i. Then, sensor node D1 computes each ratio:

$$\frac{R_{D1}^{S1}}{R_{D2}^{S1}}, \frac{R_{D1}^{S1}}{R_{D3}^{S1}}, and\ \frac{R_{D1}^{S1}}{R_{D4}^{S1}}$$

and store them in locally.

Also, at time t2, messages are broadcast by a Sybil node with a different ID this time as S2. The neighboring node from Sybil node monitors each power and reports it to the D1. This node D1 computes the ratio.

$$\frac{R_{D1}^{S2}}{R_{D2}^{S2}}, \frac{R_{D1}^{S2}}{R_{D3}^{S2}}, and\ \frac{R_{D1}^{S2}}{R_{D4}^{S2}}$$

Node D1 compares the ratios at time t1 and time t2 in order to detect the Sybil node. Node D1 concludes if the difference between two values is very close to zero, the Sybil attacking is happened in the region since received power ratio is same that indicate the same location and the message is broadcasted with multiple ID by the node. Otherwise, rejection of Sybil node by the node D1. That is, if the following equation is true then a Sybil attack is detected.

$$(\frac{R_{D1}^{S1}}{R_{D2}^{S1}} = \frac{R_{D1}^{S2}}{R_{D2}^{S2}}), (\frac{R_{D1}^{S1}}{R_{D3}^{S1}} = \frac{R_{D1}^{S2}}{R_{D3}^{S2}}), (\frac{R_{D1}^{S1}}{R_{D4}^{S1}} = \frac{R_{D1}^{S2}}{R_{D4}^{S2}})$$

3.3.2 Analysis

Demirbas's [17] proposed Sybil attack detection technique that is an efficient, lightweight and GPS free along with the consideration of limitations of wireless communication / Wireless Sensor nodes. There are a number of weaknesses in this scheme, some of which are as:

1. **Node Cooperation is Very Important**

   In this technique collaboration of some other nodes is required, collaboration of at least one is mandatory. This scheme also requires the cooperation of nodes as an important factor.

2. **The Scheme Cannot Tolerate Existing Sybil Nodes in the Network**

   They assumed an initial set of nodes whose nature is not Sybil but actually this is not the case if we are talking about real world scenario or civilian ad-hoc networks.

3. Assumed Static Network with No Mobility

Demirbas's [17] assumed WSN platform with No Mobility, i.e. Static network, where all nodes are immobile after initial deployment. The scheme is not feasible for mobile nodes or networks with mobility.

4. Collusion is not Considered

The author didn't take collusion of malicious nodes into account. Nodes may not be trusted and may collude in unfriendly hostile environment.

3.4 Jiangtao's Scheme

Sybil node detection scheme by Jiangtao et al. [18] is proposed for static clustered wireless sensor networks using RSSI and status information aggregated in the head nodes `judges the Sybil attack from received signals and status messages that are coming from the member nodes.

3.4.1 Review

In [18] Jiangtao et al. proposed a scheme that will detect the Sybil node for static clustered wireless sensor networks using RSSI and status information aggregated in the head nodes. They also used Zhong's algorithm [16] for localization. Furthermore to emulate a real network space situation, Jake's Channel Model was established between network nodes. William jakes developed a model for Rayleigh fading (it is a fading model developed specially for urban areas) based on summing a series of sinusoid signals. Two methods were proposed to enhance detection accuracy: judging member nodes and head nodes. In order to judge the nodes i.e. the member nodes, head nodes will gather information regarding the status from the member nodes and RSSi will be used for the verification of the result. Whenever a Sybil node is detected an alarm will be generated to the other node. Each head location is verified by cooperation and sharing of information by each member node. If all of the members in the group detect a Sybil head then they will generate an alarm and re-clustering will be announced. The scheme is discussed in full detail below.

A. Sybil Attack detection Method in Cluster-Based WSN

Jiangtao et al. [18] proposed Jakes channel model for WSN and then proposed a new scheme that will synthetically detect Sybil attack that is based on RSSI along with a number of parameters i.e. ID numbers, information regarding the position of nodes etc. so it will enhance the WSN security. All nodes are portioned into several numbers of clusters in the cluster based sensor network. The responsibility of allocating the bandwidth to all of the member nodes, collection / managing of data sent by each member node and data that is sent to the sink is the responsibility of the head node.

B. Jakes Channel Model of WSN

William Jakes found that Rayleigh fading process could be described by the sum of a series of complex sinusoidal signals [8]. This technology of simulating fading mobile wireless channel is called Jakes model at present, and it is applied widely in wireless communication. RSSI in the Jake channel is the function of sending and receiving distance d. The signal strength of node is:

$$RSSI_r = \frac{RSSI_t * G_{Channel}}{d^{\alpha}} = \frac{RSSI_t * \|H\|^2}{d^{\alpha}}$$

$RSSI_t$ is transmitted signal strength ($RSSI_t = 10\log P_{rec}$).

Suppose transmitted and received antenna's gain is 1, $G_{channel}$ is the channel gain which follows Rayleigh distribution. H is the impulse response of channel model. α is distance-power descending ramp, P_{rec} is node's receive power. The receive power is related with large-scale distance d, at the same time, with Jakes' channel model which obeys Rayleigh distribution.

C. Detection of Sybil Attack Based on RSSI

Jiangtao et al. [18] used Zhong‘s [16] algorithm of localization for the purpose of detection of Sybil attack. It is possible using this technique in [16]. When a message is received the four detector node will compute using equation 3 the sender location and will further associate this with the sender ID that is included in the message. Similarly when in the later stages the same location is computed along with the different sender ID then it will be a Sybil attack.

D. The Method of Detecting Sybil Attack Synthetically

Based on the neighbor’s node information that is located in the head node a threshold is selected and based on this threshold a Sybil attack is judged in the WSN. In [18] Jiangtao et al. proposed that outside intrusion in WSN in very dangerous attack (Sybil Attack). This means that outside node pretend to be an insider in order to harm the internal network. Because of different functions the method of detecting Sybil attack is different.

Like for example judging change of power and RSSI value for member nodes, multi parameter detection methods are used for the head nodes in order better accuracy improvement and refinement.

a) Algorithm for member Nodes:

Member node will exclusively communicate with one node. Given one certain member node communicate exclusively with one node. The detection methods are,

Step1. Member node denoted by v_i will send detecting information to the head node that is denoted by u_i.

$$v_i \rightarrow u_i : \{ID_{v_i}, \mathrm{Power}(v_i), \mathrm{Message}(v_i), \mathrm{Location}(v_i)\}_{u_i}$$

Step2. u_i will compares the power value and RSSI value and judge v_i

$$u_i : \{\left|\overline{\mathrm{Power}(v_i)} - \mathrm{Power}(v_i)\right| > X_P\}$$

$$u_i : \{\left|\overline{RSSI(v_i)} - RSSI(v_i)\right| > X_R\}$$

If the equation is verified then it will be a Sybil attack.

Step3. u_i will flood message in order to tell the neighbor head node u_{i+1} i=1,2…. About the detection of the Sybil attack at v_i:

$$u_i \rightarrow u_{i+1} : \{\mathrm{ID}_{u_i}; Alarm(\mathrm{v}_i), \mathrm{Location}(\mathrm{v}_i)\}_{u_i}$$

b) Algorithm for head nodes.

One head node can communicate 4 member nodes at the same time. The detection method is as,

Step1. u_i will send message (control messages) to the member node:

$$v_i : u_i \rightarrow v_i : \{\mathrm{ID}_{u_i}; Message(u_i), \mathrm{Power}(u_i)\}_{v_i}$$

Step2. Act in accordance with the RSSI value and power value sent by u_i, v_i calculate di using the equation 1. Compare d_i with d'_i which is recorded last time.

$$v_i : \{\left|d_i^{'} - d_i\right| > \mathrm{X_d}\}$$

If this equation is satisfied then v_i suppose ui is a Sybil node.

Step3. v_i send warning message to member nodes that are lying in the neighbor.

$$v_{i+1} : v_i \rightarrow v_{i+1} : \{\mathrm{Alarm}(v_i; u; 1)\} v_{i+1}$$

Step4. Node v_{i+1} detect head node again:

$$v_{i+1} : \{\left|d_{i+1}^{'} - d_{i+1}\right| > \mathrm{X_d}\}$$

If the equation above is satisfied, vi+1 result that head node is actually a Sybil node

Step5. v_{i+1} send warning message to the node v_{i+2} that is lying in the neighbor.

$$v_{i+1} \rightarrow v_{i+2} : \{\mathrm{Alarm}(\mathrm{v}_i, \mathrm{v}_{i+1}; \mathrm{u}; 2)\}_{\mathrm{v}_{i+2}}$$

The above equations verify that v_i and v_{i+1} suppose head node a Sybil node.

Step6. If $\mathrm{Alarm}(\mathrm{v}_i, \mathrm{v}_{i+1}; \mathrm{u}; 4)$ is generated, then it will indicate that 4 member nodes will verify that head node is a Sybil node.

Step7. $$\frac{RSSI_{d1}^{u1}}{RSSI_{d2}^{u1}} = \frac{RSSI_{d1}^{u2}}{RSSI_{d2}^{u2}}, \frac{RSSI_{d1}^{u1}}{RSSI_{d3}^{u1}} = \frac{RSSI_{d1}^{u2}}{RSSI_{d3}^{u2}}, \frac{RSSI_{d1}^{u1}}{RSSI_{d4}^{u1}} = \frac{RSSI_{d1}^{u2}}{RSSI_{d4}^{u2}}$$

If the above equation is satisfied then it shows that Sybil attack took place.

Step8. The new cluster will be rebuilt by the WSN so that neighbor nodes can be informed regarding the Sybil attack took place and the attacking nodes will be excluded from the network.

$$u^{'} \rightarrow uj : \{\mathrm{Alarm(u).Location(u)}\}_{u_j}$$

3.4.2 Analysis

Same number of weaknesses exists in this scheme as were found in Demirbas et al.'s [17].

1. Node Cooperation is Very Important

In this technique collaboration of some other nodes is required, collaboration of at least one is mandatory. This scheme also requires the cooperation of nodes as an important factor.

2. The Scheme Cannot Tolerate Existing Sybil Nodes in the Network

They assumed an initial set of nodes whose nature is not Sybil but actually this is not the case if we are talking about real world scenario or civilian ad-hoc networks.

3. Assumed Static Network with No Mobility

They assumed WSN platform with No Mobility, i.e. Static network, where all nodes are immobile after initial deployment. The scheme is not feasible for mobile nodes or networks with mobility.

4. Collusion is not Considered

The author didn't take collusion of malicious nodes into account. Nodes may not be trusted and may collude in unfriendly hostile environment.

3.5 Abbas et al.'s Scheme

In [7], Abbas et al. proposed a new scheme which is lightweight in the nature and in this scheme the Sybil attacker's identities are detected without the use of central trusted third party and any hardware e.g GPS.

The difference among the legitimate and Sybil node can be confirmed by the behavior of their neighboring joining. A new node i.e legitimate node will be a neighbor node as it came into the radio range of another node. The strength of the first signal that is received will be low. On the other hand, a Sybil attacker which is a neighbor already will cause to appear its new identity to be curt in the neighbor. The signal strength of the Sybil attacker is very high as compare to the newly joined node that's why Sybil attacker will be distinguished from the neighbor hat has joined recently.

Every newly joined node will be detected is the strategy and no matter the identity is used for whitewashing or a Sybil attack by the attacker.

3.5.1 Review

In order to distinguish the legitimate and the Sybil identities the RSS will be utilize in this scheme. First of all the entry / exit behavior of the node will be demonstrated for legitimate and the Sybil identity and secondly a threshold will be set to differentiate among the legitimate and Sybil identities that is based on the entry / exit behavior of the nodes in order to detect the Sybil identities. The scheme can be discussed in detail as,

A. Detection of Sybil Identities:

1. Attack Model:

There are two flavors of Sybil attacks. In the first one an attacker creates new identity while discarding its previously created one; hence only one identity of the attacker is up at a time in the network. This is also called a join-and-leave or whitewashing attack and the motivation is to clean-out any bad history of malicious activities. This attack potentially promotes lack of accountability in the network. In the second type of Sybil attack, an attacker concurrently uses all its identities for an attack, called simultaneous Sybil attack. The motivation of this attack is to cause disruption in the network or try to gain more resources, information, access, etc. Than that of a single node deserves in a network. The difference between the two is only the notion of simultaneity; however, their applications and consequences are different.

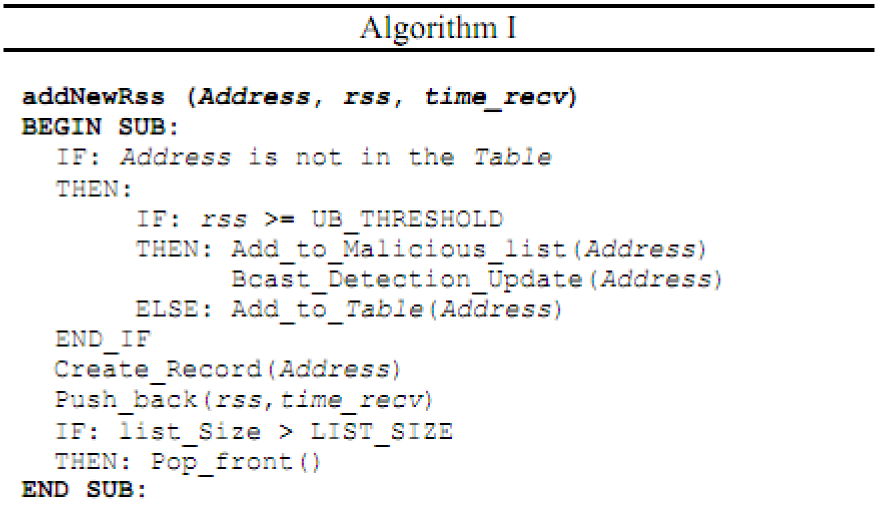
In this scheme, they consider both types of Sybil attacks. The strategy of detection mechanism is to detect every new identity created by a Sybil attacker; it does not matter if the intention of the attacker is to use that identity for whitewashing or simultaneous Sybil attacks.

2. Signal Strength Based Analysis:

A new legitimate node become neighbor as soon as they enter inside the radio range of other nodes; hence their first received signal strength at the receiver node will be low enough. In contrast a Sybil attacker, which is already a neighbor, will cause its new identity to appear abruptly in the neighborhood. When Sybil attacker creates new identity, the signal strength of that identity will be high enough to be distinguished from the newly joined neighbor.

3. Detection:

Each node maintains a list of neighbors in the form <Address, Rss-List <time, rss>>. To check the credibility of a node that either it is a legitimate node or Sybil attacker, the algorithm will checks every received RSS, along with its time of reception and the address of the transmitter. If the address is not in the RSS table, meaning that this node has not been interacted with it before, i.e. It's a new node and the RSS received is its first acknowledged presence. This first received RSS is compared against an *UB_THRESHOLD* (this threshold is used to check using the RSS whether the transmitter is in white zone, i.e. whitewasher). If it is greater than or equal to the threshold, indicating that the new node lies near in the neighborhood and did not enter normally into the neighborhood; the address is added to the malicious node list. Otherwise, the address is added to the RSS table and a link list is created for that address in order to store the recently received RSS along with its time of reception in it.



Algorithm I

```
addNewRss (Address, rss, time_recv)
BEGIN SUB:
  IF: Address is not in the Table
  THEN:
       IF: rss >= UB_THRESHOLD
       THEN: Add_to_Malicious_list(Address)
             Bcast_Detection_Update(Address)
       ELSE: Add_to_Table(Address)
  END_IF
  Create_Record(Address)
  Push_back(rss,time_recv)
  IF: list_Size > LIST_SIZE
  THEN: Pop_front()
END SUB:
```

3.5.2 Analysis

Although, Abbas et al. [7] proposed a lightweight scheme to detect the new identities of Sybil attacker without using centralized trusted third party or any extra hardware, such as directional antennae or GPS, but some weaknesses still exist in the scheme:

1. Node Cooperation is Very Important

Nodes are assumed to be cooperative and will share the recommendations honestly about other nodes. But in real world scenarios and civilian ad-hoc networks, nodes may not be cooperative and belongs to independent entities. Nodes cooperation is very important for this scheme to be feasible.

2. Cannot Detect, Prevent and Tolerate Malicious Collusion

Nodes are assumed to be trusted and cooperative. The author didn’t take collusion of malicious nodes into account. Nodes may not be trusted and may collude in unfriendly hostile environment and may share dishonest recommendations about other nodes.

3.6 Shaohe et al.’s Scheme

The scheme proposed by Shaohe et al. [19] for static sensor networks is a mechanism for detection which is called Cooperative RSSI-based Sybil Detection (CRSD) where a fixed power for all nodes is recorded. The strength of received signal is used to infer the distance between the identities in order to locate the positions of the interested type of identity using information from multiple nodes actually neighbor nodes like node cooperation. The main concept is that whatever the case is for identities the physical location will be the same for identities that are claimed by the Sybil node. So the Sybil attack will be detected in a reasonable suspect if the physical location is same for a number of different identities. A Sybil attack will be in place if more number of such is exists. The Sybil node can be detected in a number of ways; one way is that CRSD is making use of the exact position of the nodes. The position can be find using the below mathematical equation where d is the distance calculated by d(S, D) and b is the attenuation. The received signal will be calculated as,

$$RSS_{S-D} = C_e * d(\mathrm{S},\mathrm{D})^{-b} * RSS_S$$

Consider the communication between node A and two Sybil identities S1 and S2. According to our assumption, one have RSS_{S1}=RSS_{S2} and d(S1,D)= d(S2,D). So RSS_{S1-D}=RSS_{S2-D}. CRSD therefore group the identities with similar RSS together to detect Sybil identity.

If only the RSS from one node is used, however, the frequency of false positive is high means detection Sybil identity by single node is inefficient, i.e. RSS from a single node is insufficient.

The other method according to Shaohe et al. [19], RSS will determine the distance across the nodes but won’t specify the position in two dimensional space but can determine position in the three dimension space. This thing can be exploited by the CRSD to find the position if the desired identity. CRSD will require cooperation among the neighbor nodes in order to find the position of the desired identity.

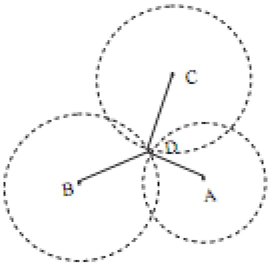
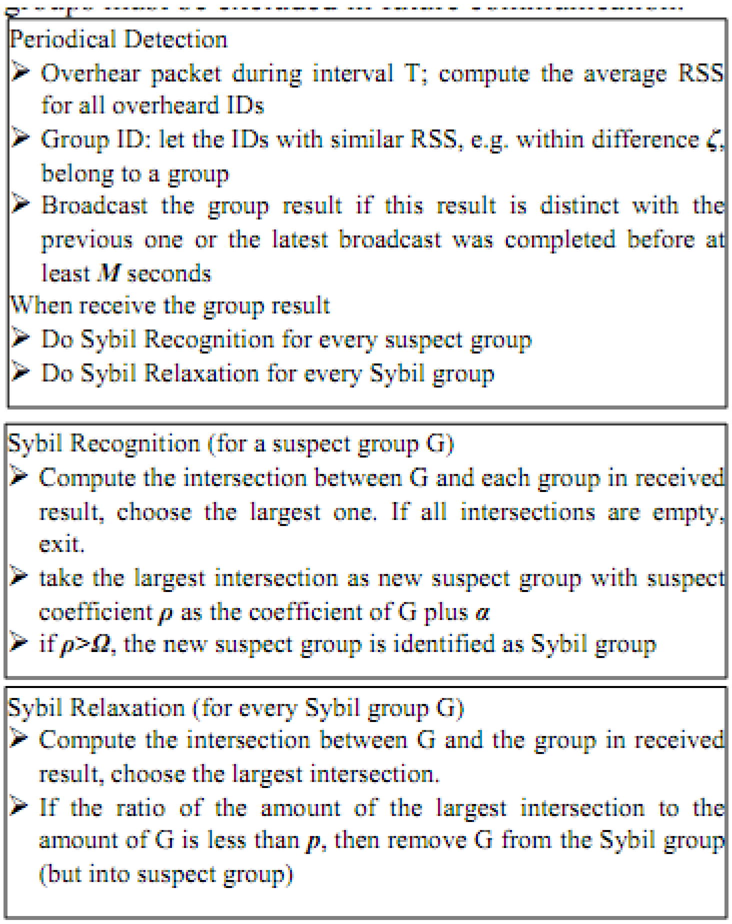


Fig.2 The position of D is determined by the distances from D to at least three nodes that not settle at the same line

CRSD [19] will not rely on position but on the relationship that exists between the identities. If there are multiple of the nodes that are having similar distance lying to them then we can say that these nodes are having the same position. This kind of group will be a Sybil attack and will be a false positive.



Periodical Detection

- Overhear packet during interval T; compute the average RSS for all overheard IDs
- Group ID: let the IDs with similar RSS, e.g. within difference ζ, belong to a group
- Broadcast the group result if this result is distinct with the previous one or the latest broadcast was completed before at least M seconds

When receive the group result

- Do Sybil Recognition for every suspect group
- Do Sybil Relaxation for every Sybil group

Sybil Recognition (for a suspect group G)

- Compute the intersection between G and each group in received result, choose the largest one. If all intersections are empty, exit.
- take the largest intersection as new suspect group with suspect coefficient ρ as the coefficient of G plus α
- if $\rho > \Omega$, the new suspect group is identified as Sybil group

Sybil Relaxation (for every Sybil group G)

- Compute the intersection between G and the group in received result, choose the largest intersection.
- If the ratio of the amount of the largest intersection to the amount of G is less than p, then remove G from the Sybil group (but into suspect group)

3.6.1 Analysis

This research thesis proves that Shaohe et al. [19] Sybil attack detection scheme can be easily defeated through malicious Collusion between nodes. A group of colluded nodes can disrupt all the detection process. Colluded group can detect benign nodes as Sybil. Some weaknesses in the scheme are as under:

1. Node Cooperation is Very Important for the Scheme to be Viable

Nodes are assumed to be cooperative and will share the exact distances honestly about other nodes. But in real world scenarios, nodes may not be cooperative and can be selfish. Nodes cooperation is very important for this scheme to be feasible. Because, without nodes cooperation, nodes position cannot be located for Sybil identity detection.

2. Cannot Tolerate Collusion

Nodes are assumed to be trusted and cooperative. The author didn’t take collusion of malicious nodes into account. Nodes may not be trusted and may collude in unfriendly hostile environment and may share dishonest recommendations or fake distance information about other nodes.

3. Overhead and Resource Consumption

The scheme broadcasts group results which are too costly in terms of memory and this communication can significantly exhaust the sensors’ batteries.

4. Works only for Static Network

The scheme works only in Static environment. Not feasible for mobile networks.

3.7 Xiao et al.’s Scheme

In order to detect the Sybil attack in the VANET Xiao et al. [22] proposed a scheme. This scheme will take advantages of the pattern of VANET traffic and roadside base stations. This a distributed approach as well as localized approach which make use of the strength of the signals using some statistical analysis and will be under observation for a certain amount of time. The claimed position can be verified by each node on the road in order to detect the Sybil node. First of all a basic signal-strength-based position verification scheme has been introduced however it is still vulnerable to a number of different spoof attacks. In order to compensate the vulnerabilities Sybil nodes prevention techniques are introduced.

Xiao et al.’s [22] scheme is discussed as follows:

1. BASIC SIGNAL STRENGTH BASED POSITION VERIFICATION:

In this section, Xiao et al propose a basic scheme for verifying position claims by signal strength analysis. Verification scheme relies on monitoring the signal strength of periodical beacons. For clarity of description, [22] define three categories of nodes’ roles: claimer, witness, and verifier. Each node would periodically play all these roles, that is, each node is a claimer, a witness as well as a verifier but at various moments and for various purposes.

Claimer: Each node periodically broadcasts a beacon message at beacon intervals, for the purpose of neighbor discovery. At this moment, we name the node as a claimer.

Witness: All neighboring nodes, within the signal range of the claimer, would receive the previous beacon message. They measure the signal strength and save the corresponding neighbor information in their memory.

Verifier: After receiving a beacon message, a node waits for a verifying interval, during which it collects enough signal strength measurements concerning the previous beacon message from neighboring witnesses.

With the collected measurements, the node can locally compute an estimated position of the claimer, for example, by performing MMSE (Minimum Mean-Square Error) on the collected signal strength and a pre-defined radio model. To obtain the estimated position, we first calculate the mean square error:

$$MSE_{(\mathrm{p})} = \frac{\sum_{i=1}^{k} (S_r(\mathrm{w}_i) - S_m(\mathrm{w}_\mathrm{i}, \mathrm{p}))^2}{k}$$

If the estimated position of a claimer is far away from its claimed position, it is regarded as a suspect node.

2. DETECTING SYBIL NODES IN VANETS:

In this section, [22] propose a detection scheme for ensuring that each physical vehicle is bound with only one identity. If multiple identities, claiming to be at various positions, prove to be at one physical position through position verification, then Sybil attacks are likely in progress.

The detection model specifies which nodes are potential Sybil nodes. Formally, let ν be the set of all vehicles and let S be the set of sets of Sybil nodes. The model is a function D: ν → S. We classify two Sybil nodes into one set, if they originate from one physical vehicle. The function, D, can be implemented by any cluster algorithm. However, the challenge is how to detect a Sybil node and how to decide the correlation between two potential Sybil nodes.

The overall detection process, performed by each node, includes three phases:

- **Phase 1:** Node v periodically broadcasts beacon messages and receives beacon messages from neighboring nodes. The corresponding signal strength measurement for each received beacon message is saved in its memory.
- **Phase 2:** When node v collects enough signal strength measurements for a neighboring node, s, node v performs the enhanced position verification algorithm on s.
- **Phase 3:** If s proves to be a Sybil node in Phase 2, node v performs the Sybil node classification algorithm on s and other neighboring nodes, attempting to find all potential Sybil nodes originating from the same malicious physical node.

3.7.1 Analysis

Xiao et al.'s [22] proposed an efficient scheme for Sybil attack detection for VANETs, with mobility as taken into account. But there are some security flaws in this scheme. Some of the weaknesses in the scheme are as discussed below:

1. Additional Hardware Required

Each vehicle will be equipped with GPS devices, and GPS positions are supposed to be accurate.

2. Vehicles are assumed to be Trusted

It is assumed that most drivers (vehicles) will be trusted; however this is not a situation in the real world scenarios.

3. Roadside Base Stations

It is assumed that roadside base stations are sparsely deployed along roads, and the identity authentication infrastructure such as ELP (Electronic License Plate) has been implemented for the whole network. Without the support of roadside base stations, the scheme won't work efficiently.

4. Susceptible to Collusion Attack

The scheme is susceptible to witness based collusion attack by witnesses and verifiers. Most of the vehicles are assumed to be trusted however nodes can Collude in unfriendly hostile environment.

To the best of our knowledge, there is no formal model of accurately detecting Sybil attacks in the presence of malicious collusion and detecting and excluding those colluding nodes, analysis of the level of encounter risk of malicious collusion on the detection accuracy of Sybil attacks in MANETs. A successful collusion attack often works on the principle that nodes shows itself as reliable and trustworthy and cooperate in some type of interactions, usually direct interaction and then deceive the node in witness interaction, i.e. providing false information about other nodes to support colluding group or defame or degrade other benign nodes. This forged information promotes the colluding group and the victims will interact with it and will be betrayed. This lack of study on witness-based collusion attacks while cooperative detection of Sybil attacks motivates the work reported in this thesis.

Our contributions include the introduction of witness-based collusion attacks in the detection of Sybil attacks in MANETs; an analysis of the impact of malicious collusion on Sybil attack detection in MANETs; and development of a novel and robust trust based Sybil attack detection scheme resistant to collusion and incorporating trust based mechanism that would mitigate the benefit (the payoff gained from collusion) transfer among nodes.

3.8 Conclusion

It is clear from the above discussion that all the localization and RSSI based Sybil attack detection schemes need the cooperation of other nodes to detect Sybil attack accurately. But the main problem in node cooperation is that in civilian ad hoc networks, nodes often belong to different individuals and have their own interests. Consequently, nodes may not always behave cooperatively and may collude in such environments and can disseminate false location information for disrupting the detection accuracy of such systems. This thesis research proved that even the most recently proposed lightweight Sybil attack detection scheme i.e. Abbas et al. [7] fails to detect Sybil attack accurately in the presence of malicious colluding nodes. It is also clear from the above discussion that if the assessor node bases evaluation of other nodes on the basis of cooperation in direct associations, the collusion attack will be successful and the scheme won’t be able to detect Sybil nodes accurately.

Chapter 4

PROPOSED APPROACH FOR COLLUSION RESISTANT SYBIL ATTACK DETECTION

4.1 Introduction

Trust is one of the most crucial concepts driving decision making and establishing relationships. Trust is indispensible when considering interactions among decentralized nodes in MANETs. According to Jarvenpaa et al. [30], trust is an essential aspect of any relationship in which the trustor does not have direct control over the actions of a trustee, the decision is important, and the environment is uncertain. Trusted relationships among nodes in a network are based on different sources of information such as direct interactions, witness information and previous behaviors of nodes. Trust management in distributed and resource-constraint networks, such as disconnected mobile ad-hoc networks (MANETs) and sensor networks, is much more difficult but more crucial than in traditional hierarchical architectures, such as the Internet and access point centered wireless LANs. Generally, this type of distributed network has neither pre-established infrastructure, nor centralized control servers or trusted third parties.

This research work is based on Sybil attack detection in Mobil ad hoc networks by analyzing RSSI of each new node or ID in the network, specifically in the presence of collusion attack or malicious colluding nodes which can disrupt the detection accuracy of Sybil nodes. The focus remains on the revealing of malicious or selfish colluding nodes while detecting Sybil nodes with special attention to incorporating trust based mechanism that would mitigate the benefit (the payoff gained from collusion) transfer among nodes. This notion of trust will act as an incentive for nodes which will motivate nodes to cooperate.

Our work is related to the improvement of the ‘Lightweight Sybil attack detection scheme [7]’ that is used ultimately to detect and separate the malicious Sybil nodes from the network. Furthermore a collusion detection scheme have been proposed to work as an extension of [7] to accurately detect Sybil identities and expose and exclude the malevolent colluding nodes from the network. Likewise, our ‘Collusion-resistant Sybil attack detection scheme”, described in Chapter 4, is an extension of the ‘Lightweight Sybil attack detection scheme [7]’. Abbas et al. [7] have undertaken a performance comparison of other RSSI based popular Sybil detection schemes and have established the result that [7] has the best throughput performance and accuracy; assuming nodes are cooperative with no malicious collusion. This motivates us to use [7] as the basic Sybil detection Scheme for our proposed work.

Our contributions include the introduction of witness-based collusion attacks in the detection of Sybil attacks in MANETs; an analysis of the impact of malicious collusion on Sybil attack detection in MANETs; and development of a novel and robust trust based Sybil attack detection scheme resistant to collusion and incorporating trust based mechanism that would mitigate the benefit (the payoff gained from collusion) transfer among nodes. This proposed scheme is designed to calculate trustworthiness of each node, analyze the behavior pattern of nodes, detect, and thwart collusion and Sybil attacks. This chapter presents all the details of proposed scheme to detect a Sybil attack in a collusion resistant manner. Detect the new identities of Sybil attacker without using centralized trusted third party or any extra hardware, such as directional antennae or GPS.

4.2 Proposed Scheme

The proposed scheme is designed to calculate trustworthiness of each node, analyze the behavior pattern of nodes, detect, and thwart collusion and Sybil attacks. There is no need of designated and honest monitors to perform the Sybil attack detection. Each mobile node in the network observes packets passing through it and periodically exchanges its observations in order to determine the presence of an attack. Malicious nodes fabricating false observations will be detected and rendered ineffective. The motivation for having two types of trust, i.e. Direct and Indirect trust, is that we believe trustworthiness has different independent dimensions. For instance, a node that is trustworthy in a direct interaction is not necessarily trustworthy in a witness interaction. The main objective of indirect trust computation is to determine the trustworthiness of a (unfamiliar) node from the set of recommendations that narrow the gap between the derived recommendation and the actual trustworthiness of the target node for detecting collusion.

There are some goals that are considered to be achieved while designing the proposed Sybil attack detection scheme. The goals include the following:

- Collusion resistant; the scheme should have a reasonable tolerance against collusion
- Detect the new identities of Sybil attacker without using centralized trusted third party or any extra hardware, such as directional antennae or GPS
- Trust value will be linked with nodes behavior, i.e. Trust value increases with good actions and decreases with bad actions on the basis of "Trust is hard to earn but easy to lose”
- Supports good trust history

The scheme works as follows:

4.2.1 Trust Value Calculation

Nodes interact with each other; every node gives a rating to another node’s performance and stores the history. Every node will calculate a Trust value for every other with the technique used in the FIRE [27].

$$T_{(a,b)} = \frac{\sum_{ri \in R(a,b)} \omega_{(ri)} . v_i}{\sum_{ri \in R(a,b)} \omega_{(ri)}}$$

Where $T_{(a,\ b)}$ is trust variable, *a* is an evaluator node, *b* is a target node. $T_{a,b}(t) \epsilon [0, 1]$ and $T_{a,b}(0) = 0.5$; Where *t* is the number of interactions, $R_{(a,b)}$ is the set of ratings for calculating $T_{(a,b)}$. $\omega_{(ri)}$ is the weight corresponding to r_i. The weight $\omega_{(ri)}$ for each rating is selected such that it gives more weight to more recent ratings, with a constraint

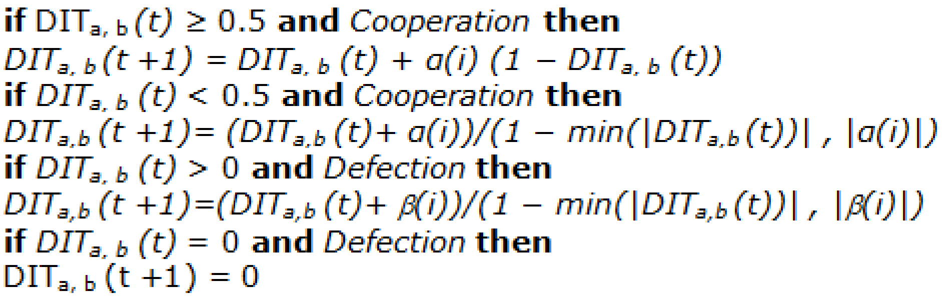
$$\sum_{r_i \in R(a,b)} \omega_{(ri)} = 1$$

The value of $\omega_{(ri)}$ must be greater or equal to *0 (zero)* and *vi* is the rating of *ri*; The range of v_i is [0, 1], where 0 means absolutely negative or Complete Uncertainty, 1 means absolutely positive or total confidence, and 0.5 means neutral or uncertain. Where t is the current time and t_k is the time on which the interaction took place.

$$\omega_{ri} = e^{-\frac{\vartriangle t(\mathrm{ri})}{\lambda}}$$

$$\omega_{ri} = e^{-\frac{t-t_k}{\lambda}} \quad \textbf{And} \quad \lambda = \frac{-5}{\ln(0.5)}$$

The trust value for target node (n_b) is updated on the basis of positive (α) and negative (β) number of interactions using the following rules defined in [28]:



```
if $DIT_{a,b}(t) \geq 0.5$ and Cooperation then
$DIT_{a,b}(t+1) = DIT_{a,b}(t) + \alpha(i)\,(1 - DIT_{a,b}(t))$
if $DIT_{a,b}(t) < 0.5$ and Cooperation then
$DIT_{a,b}(t+1) = (DIT_{a,b}(t) + \alpha(i))/(1 - \min(|DIT_{a,b}(t))|, |\alpha(i)|)$
if $DIT_{a,b}(t) > 0$ and Defection then
$DIT_{a,b}(t+1) = (DIT_{a,b}(t) + \beta(i))/(1 - \min(|DIT_{a,b}(t))|, |\beta(i)|)$
if $DIT_{a,b}(t) = 0$ and Defection then
$DIT_{a,b}(t+1) = 0$
```

The values of α = 0.3 and β = -0.1 and cooperation means value of $v > 0.5$ and defection means $v < 0.5$.

4.2.2 Sybil Node Detection

In order to detect a Sybil node we will use the technique by Abbas et. al [7]. To check the credibility of a node that either it is a legitimate node or Sybil attacker, an algorithm will checks every received RSS, along with its time of reception and the address of the transmitter. If the address is not in the RSS table, meaning that this node has not been interacted with it before, i.e. it's a new node and the RSS received is its first acknowledged presence. This first received RSS is compared against an *UB_THRESHOLD* (this threshold is used to check using the RSS whether the transmitter is in white zone, i.e. whitewasher). If it is greater than or equal to the threshold, indicating that the new node lies near in the neighborhood and did not enter normally into the neighborhood;

4.2.3 Collusion detection

Our Scheme works as follows:

The proposed method is designed to calculate trustworthiness of every node, detect and thwart collusion and Sybil attacks. Instead of designated nodes, the packets passing through the network are monitored by every mobile node and the observations will be exchanged for the detection of the Sybil and attacks. False recommendations that are produced by the malicious nodes will be detected and made ineffective. We have defined two types of trust, i.e. direct interaction trust and indirect interaction trust. The idea of having two types of trust is that we believe trust has different independent aspects. For example, a node that is trustworthy in a one type of interaction, i.e. direct interaction, is not undoubtedly trustworthy in indirect (witness) interaction.

Each node maintains a list of neighbors in the form ***<Address, Rss-List <time, rss>>***, and records the RSS values of any directly received or overheard frames of 802.11 protocol i.e. RTS, CTS, DATA and ACK messages. In other words, each node will capture and store the signal strength of the transmissions received from its neighboring nodes. This can be performed when a node either takes part in the communication directly with other nodes acting as a source or a destination or when a node does not take part in the direct communication.

Our approach works as follows:

- Nodes interact with each other; every node gives a rating to another node’s performance and stores the history. Every node will compute a Trust value (recommendation) for every other node with the technique used in the FIRE [27]. Trust values stores in a table in the form:

  $$Hi \;=\; \left\{ Direct\,/\;\; Indirect,\; n_j,\; T_{i,j},\; ttl \;\right\}$$

  Where *Direct/ Indirect* means that the value is from direct interaction or from witness nodes, n_j is the target node, $T_{i,j}$ is trust value of node n_j in the range *[0, 1], ttl* is the time stamp when the trust value is determined.

- **Case 1:** To check the credibility of a node that either it is a legitimate node or Sybil attacker, upon detection of new RSS (by evaluator node), node will check the nodes’ address in Table ***<Address, Rss-List <time, rss>>*** to verify the received RSS, its reception time and the transmitter address**.** If address is in the Table, then benign node and add RSS value to the table. If the address of the interacting node is not in the RSS table, means that this is the first interaction of the node and the RSS received is its first acknowledged presence.

- Compare RSS with '*RSS_UB_THRESHOLD*'. This threshold determines the node penetrated normally, i.e. new node, or already a node present in the neighborhood in case if it's RSS is greater than or equal to the threshold. If *RSS >= RSS_UB_THRESHOLD*, then Add node ID to Malicious node list as Sybil ID. We are using the technique by Abbas et. al [7].

- Then evaluator node will ask for Recommendations about the target node.

- Evaluator node will Sort & Analyze the Recommendations according to the method defined by Iltaf et. al [5].
  - Finding Dissimilarity of every Recommendation Received
  - Finding Smoothing Factor (SF) for determining the set of dishonest (colluding) recommendation classes from the set of all recommendations.
  - Concluding and Separating Dishonest Recommendation class and its Recommenders (the malicious colluders)
- **Case 2:** If a node gets Sybil detection update packet from another node which is out of radio range of the evaluator node, i.e. node that received the Sybil detection update packet.
  - **Condition I:** If evaluator node receives the same detection packet from more than two trusted nodes, then; node target node will be added to malicious nodes list.

  - **Condition II:** But, if the detection update packet is from two or less than two nodes (or from untrusted nodes), then evaluator node will also request for recommendations about node target node.
- Again the evaluator node will Sort and Analyze the received recommendations, find dissimilarity values of every recommendation, calculating smoothing factor to determine the set of dishonest (colluding) recommendation class and finally

concluding and separating Dishonest Recommendation class and its Recommenders (the malicious colluders).

- Malicious colluding nodes can provide two types of dishonest recommendations:
  - Colluding nodes can launch **Ballot stuffing attack** in which the intention of the attacker is to send malicious recommendations that will cause the evaluated trustworthiness of an entity to increase. Means they will give high ratings about the Sybil identity to promote it as a trustworthy user to defraud other users and to maximize the utility of the colluding group.

  - They can launch **Bad mouthing attack** in which the intention of the attacker is to send malicious recommendations that will cause the evaluated trustworthiness of an entity to decrease. Means they will defame other trustworthy nodes by promoting them as Sybil or untrustworthy nodes to isolate it from the network, again, to defraud other users and to maximize the utility of the colluding group.

The above explanation means that there will be a wide discrepancy between the recommendations provided by the colluding group and trustworthy nodes.

4.2.4 Working Examples

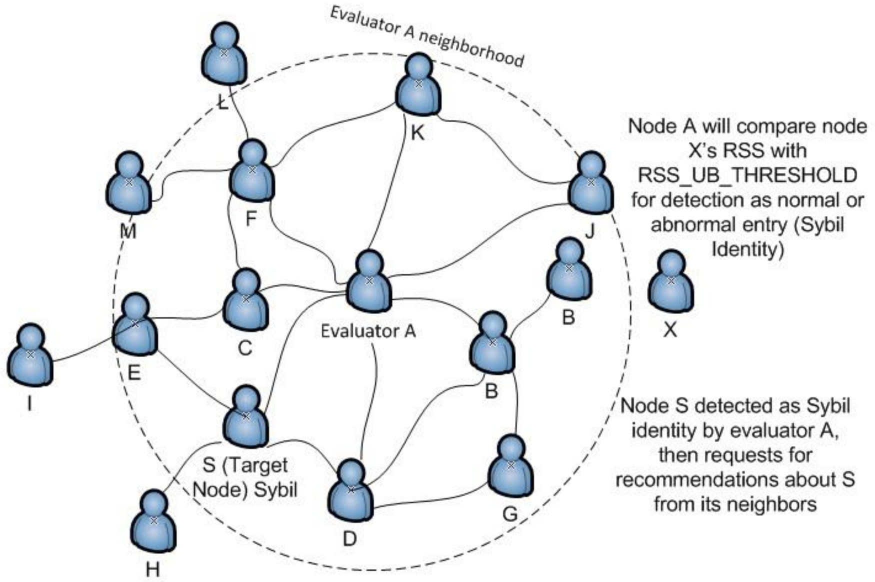
Here are two working examples of our proposed approach.

a) Example I: Direct Detection of Colluding Nodes

Let a node (S) has been detected as Sybil by the evaluator node A (and at least 1 or 2 other nodes). Before sending a detection update packet; Node A will request for recommendation/ trust values about node S (the Sybil node). Naturally, benign nodes will share actual values of node S, i.e. as distrusted malicious node with low trust values or their will be no recommendations from trusted benign nodes (because of newly created Sybil identity with no previous records); but, malicious ‘colluded’ nodes, i.e. node in collusion with S, will give high ratings for node S. So these nodes (considered) are/ will be definitely in collusion with the Sybil/ malicious node (S), i.e. malicious nodes and Sybil node (S) may collude in order to produce false positive recommendation to the evaluator and at the same time promoting the malicious target as a trusted user. These (colluded) nodes will also be added to distrusted nodes list and their trust value will be decremented. This technique will thwart witness based collusion attack. After this a detection update packet will be send to one-hop neighbors.

Ballot Stuffing Attack: is one in which the intention of the attacker is to send malicious recommendations that will cause the evaluated trustworthiness of an entity to increase.

After this a detection update packet will be send to one-hop neighbors.



Node A will compare node X's RSS with RSS_UB_THRESHOLD for detection as normal or abnormal entry (Sybil Identity)

Node S detected as Sybil identity by evaluator A, then requests for recommendations about S from its neighbors

Figure 4.1: Example I: Direct detection of Colluding nodes

b) Example II: Indirect Detection of Colluding Nodes

Let node A get a Sybil detection packet from node C (broadcast upon detection of Sybil identity) about node S (out of radio range of A).

Condition I: If node A receives the same detection packet from more than two (n>2) trusted nodes (T > 0.5), then; node S will be added to malicious nodes list.

Condition II: But, if the detection update packet is from two or less than two nodes (or from untrusted nodes, T<0.5), then node A will request for recommendations about node S.

If node S is a Sybil node (i.e. majority of the nodes consider it Sybil/ distrusted), other trustworthy nodes will give the same values as node C and other nodes. However, Nodes that will collude with node C and S, i.e. the Colluding group, will give false recommendations, i.e. high ratings about the Sybil identity S to promote it as a trustworthy user to defraud other users and to maximize the utility of the colluding group.

In other case, let suppose C is a malicious node and S is a benign node; then C can defame S to isolate it from the network.

Thus there will be a wide discrepancy between the recommendations provided by the colluding group and trustworthy nodes. Users in the colluding group may adopt a sacrificial stance in the collusion attacks for the purpose of maximizing utility of colluding group.

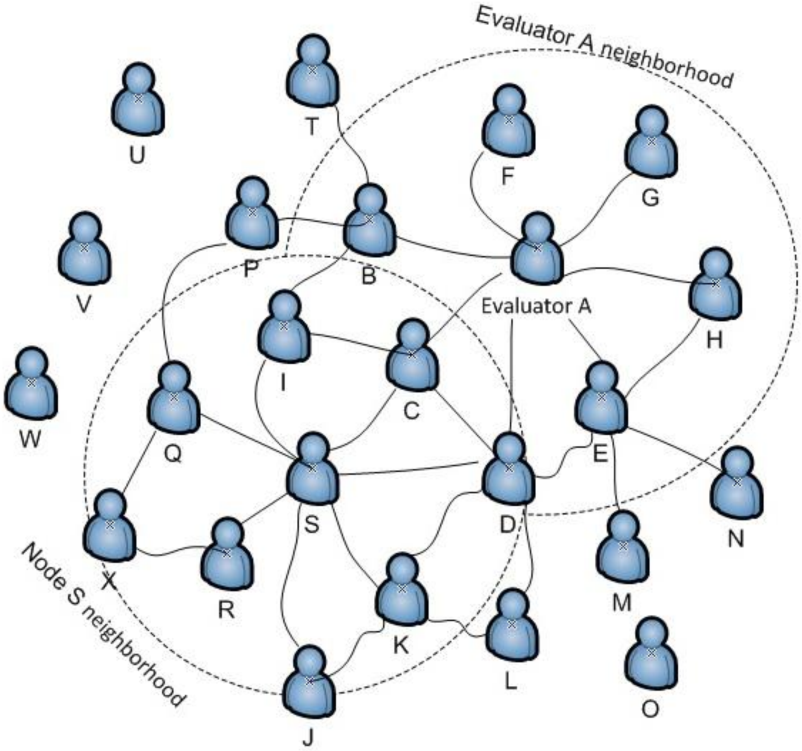


Figure 4.2: Example II: Indirect detection of Colluding nodes

The addresses are then appended to malicious node list. Otherwise a new record has been created for the new node and added to the RSS table with received RSS and reception time.

4.2.4 Algorithm for Collusion Detection

Our proposed scheme will detect Sybil nodes in a collusion resistant manner. To check that either the node is legitimate or Sybil attacker, an algorithm will checks every received RSS, along with its time of reception and the address of the transmitter. If the address is not in the RSS table, meaning that this node has not been interacted with it before, i.e. It's a new node and the RSS received is its first acknowledged presence. This first received RSS is compared against an UB_THRESHOLD (this threshold is used to check using the RSS whether the transmitter is in white zone, i.e. whitewasher). If it is greater than or equal to the threshold, indicating that the new node lies near in the neighborhood and did not enter normally into the neighborhood. For detecting nodes in collusion and disrupting the MANET, our proposed algorithm will make a decision on the basis of recommendations, i.e. if a recommendation is far from the median value of a given recommendation set and has a lower frequency of occurrence; it is filtered out as a dishonest recommendation.

Suppose that an evaluator node n_i need to find the trust value of node n_j. If node n_i has no previous interaction history with node n_j, it will broadcast the request for recommendations for node n_j. Let R denote the set of recommendations collected from recommenders.

$$R = \{r_1,\ r_2,\ r_3,\ ......\ ,\ r_n\}$$

We divide the range of possible recommendation values into *b* intervals (or bins).

$$H(R) = \{(\mathrm{Rc}_1, \mathrm{f}_1), (\mathrm{Rc}_2, \mathrm{f}_2), (\mathrm{Rc}_3, \mathrm{f}_3), (\mathrm{Rc}_4, \mathrm{f}_4), (\mathrm{Rc}_5, \mathrm{f}_5), (\mathrm{Rc}_6, \mathrm{f}_6), (\mathrm{Rc}_7, \mathrm{f}_7), (\mathrm{Rc}_8, \mathrm{f}_8), (\mathrm{Rc}_9, \mathrm{f}_9), (\mathrm{Rc}_{10}, \mathrm{f}_{10})\}$$

Where f_i is the total number of recommendations falling in R_{ci}. From this histogram H(R), we remove all the recommendation classes with zero frequencies and get the domain set (Rdomain) and frequency set (f).

$$Rdomain = \{\mathrm{Rc}_1, \mathrm{Rc}_2, \mathrm{Rc}_3, ..., \mathrm{Rc}_{10}\}$$
$$f = \{f_1, f_2, f_3, ..., f_{10}\}$$

<u>Dissimilarity Function</u>: The dissimilarity function $\mathrm{DF}(x_i)$ is defined as

$$\mathrm{DF}(x_i) = \frac{|\, x_i - median(\mathrm{x})\,|^2}{f_i}$$

Where x_i is a recommendation class from a recommendation set *x*. Under the proposed approach, the dissimilarity value of xi is dependent on the square of absolute deviation from the median,

$$i.e, |\, x_i - median(\mathrm{x})\,|^2$$

For each R_{ci}, a dissimilarity value is computed using Equation 1 to represent its dissimilarity from the rest of the recommendations with regard to their frequency of occurrence. All the recommendation classes in *Rdomain* are then sorted with respect to their dissimilarity value DF(R_{ci}) in descending order. The recommendation class at the top of the sorted *Rdomain* with respect to its DF(x_j) is considered to be the most suspicious one to be filtered out as dishonest recommendation. Once the *Rdomain* is sorted, the next step is to determine the set of dishonest recommendation classes from *Rdomain* set. To help find the set of dishonest recommendation classes from the set of recommendations in *Rdomain*, Arning et al. [29] defined a measure called smoothing factor (SF):

<u>Smoothing Factor (SF)</u>: A SF for each $SRdomain$ is computed as:

$$SF\left(SRdomain_j\right) \;=\; C\left(Rdomain \;-\; SRdomain_j\right) \;\times\; \left(DF\left(Rdomain\right) \;-\; DF\left(SRdomain_j\right)\right)$$

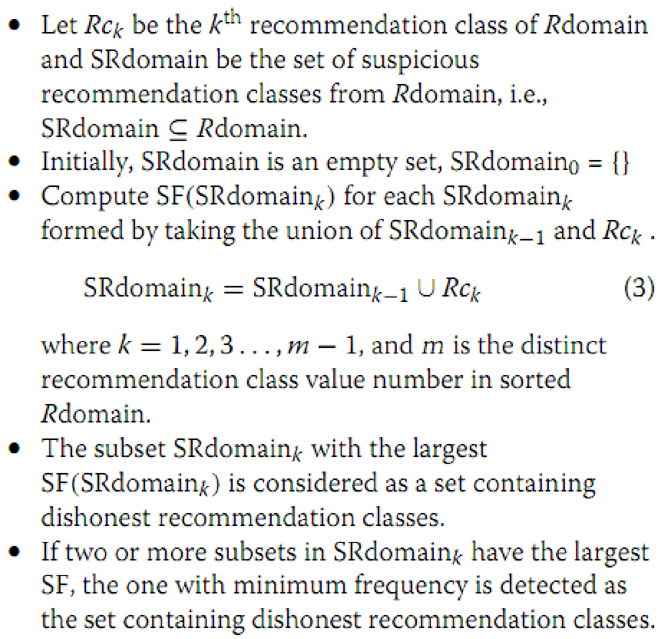
Where $j \;=\; 1,\; 2,\; 3\; ...,\; m,$ and m is the total number of distinct elements in SRdomain. C is the cardinality function and is taken as the frequency of elements in a set $\left\{Rdomain \;-\; SRdomain_j\right\}$. The SF indicates how much the dissimilarity can be reduced by removing a suspicious set of recommendation (SRdomain) from the Rdomain.

<u>Dishonest Recommendation Domain</u>: The dishonest recommendation domain $\left(Rdomain_{dishonest}\right)$ is a subset of Rdomain that contributes most to the dissimilarity of Rdomain and with the least number of recommendations, i.e., $Rdomain_{dishonest} \subseteq Rdomain$. We say that $\mathrm{SRdomain}_x$ is a set of dishonest recommendation classes with respect to SRdomain, C, and DF($\mathrm{SRdomain}_j$) if

$$SF\left(SRdomain_x\right) \;\geq\; SF\left(SRdomain_j\right)\; x,\; j \in m$$

for all Rdomain, C, and SRdomain$_j$.

In order to find out the set of dishonest recommendation $Rdomain_{dishonest}$ from Rdomain, we use the mechanism defined by Iltaf et. al[5]:



- Let Rc_k be the k^{th} recommendation class of Rdomain and SRdomain be the set of suspicious recommendation classes from Rdomain, i.e., SRdomain $\subseteq$ Rdomain.
- Initially, SRdomain is an empty set, SRdomain$_0$ = {}
- Compute SF(SRdomain$_k$) for each SRdomain$_k$ formed by taking the union of SRdomain$_{k-1}$ and Rc_k .

$$\text{SRdomain}_k = \text{SRdomain}_{k-1} \cup Rc_k \qquad (3)$$

  where $k = 1, 2, 3 \ldots, m - 1$, and m is the distinct recommendation class value number in sorted Rdomain.
- The subset SRdomain$_k$ with the largest SF(SRdomain$_k$) is considered as a set containing dishonest recommendation classes.
- If two or more subsets in SRdomain$_k$ have the largest SF, the one with minimum frequency is detected as the set containing dishonest recommendation classes.

After detecting the set $Rdomain_{dishonest}$, we remove all recommendations that fall under the dishonest recommendation classes. **These will be colluding classes**.

```
Require:
1. RSS
2. Set of Recommendations
Ensure:
1. Sybil ID detection (If RSS>Threshold)
2. Rdomain_dishonest [Colluding Nodes]

Step 1:   addNewRss (Address, rss, time_recv)
Step 2:   Begin Sub
Step 3:   if address is not in the Table then
Step 4:   if rss >= RSS_UB_THRESHOLD then
Step 5:   Add_to_Malicious_list (Address) And
              OR
              if Got Sybil detection update packet
              Check for address (records)
              If Address is not in the Table // Record not found
              Then // ask for recommendation
/* Collusion detection by sorting out dishonest recommendation
Ask for recommendations*/
Step 6: for i = 1 → 10 do
Step 7: $Rc_i = i/10$
Step 8: $f_i$ = number of recommendations in interval [i/10 − 0.1, i/10]
Step 9: end for
Step 10: for i = 1 → 10 do
Step 11: if $f_i$ <> 0 then
Step 12:         Rdomain[k] = $Rc_i$
Step 13:         H [k ++] = {Rci, $f_i$}
Step 14: end if
Step 15: end for
Step 16: $\bar{x}$ = Median (Rdomain)
Step 17: for each k in Rdomain do
Step 18: $DF(x_i) = \frac{|Rdomain[k]-\bar{x}|^2}{f_k}$ //calc deviation
Step 19: end for
Step 20: SRdomain = SortDesc (Rdomain, DF)
Step 21: D0 =∅
Step 22: for j = 1 to size of (SRdomain) - 1 do
Step 23: $D_i \cup (SRdomain_j)$
Step 24: $SF_k$ = SmoothingFactor ($D_j$)
Step 25: end for
Step 26: $SF_{max} = max(SF(D_k))$
Step 27: $f_{min}$ = min freq of k in SRdomain with SF = $SF_{max}$
Step 28: $Rdomain_{dishonest}$ = all k in SRdomain with SFk = $SF_{max}$ and $f_k$ = $f_{min}$
Step 29: return $Rdomain_{dishonest}$
Step 30:   Bcast_Detection_Update (Address)
Step 31: else
Step 32: Add_to_Table (Address)
Step 33: End_If
Step 34:   Create_Record (Address)
Step 35:   Push_back (rss, time_recv)
Step 36: if list_Size > LIST_SIZE then
Step 37: Pop_front ()
Step 38: End Sub
```

Algorithm 1

4.2.4.1 Step-by-Step Process of ‘Collusion-Resistant Sybil Attack Detection’

In order to detect the Sybil and Colluded nodes, the mechanism defined by the proposed approach is as follows:

- Let $T_{(a, b)}$ is trust value node a (a is an evaluator node) has on node b (b is a target node)

```
Step1: Case 1➔for each new RSS do
Check Address in Table
If address is in the Table
Then: Benign node ➔Add to table
Else

Step 2: Compare RSS with ‘RSS_UB_THRESHOLD’
If RSS >= RSS_UB_THRESHOLD
Then: Add to Malicious node list as Sybil ID ‘And’

Step 3: Ask for Recommendations
Step 4: Sort & Analyze the Recommendations
Step 5: Finding Dissimilarity of every Recommendation Received
Step 6: Finding Smoothing Factor (SF): To determine the set of dishonest
recommendation classes from the set.
Step 7: Concluding and Separating Dishonest Recommendation Domain and its
Recommenders
Case 2➔If Got Sybil detection update packet
                Then
        Check for address in table
        If Address is not in Table
        Repeat the following Steps
Step 3: Ask for Recommendations
Step 4: Sort & Analyze the Recommendations
Step 5:  Finding Dissimilarity of every Recommendation Received
Step 6:  Finding Smoothing Factor (SF): To determine the set of dishonest
recommendation classes from the set.
Step 7:  Concluding and Separating Dishonest Recommendation Domain and its
Recommenders
```

Result: Finally, the set of dishonest recommenders or colluded nodes will be separated and add to malicious table

4.2.5 Recommended Trust Value

The final trust value (Recommended Trust Value) will be:

After computing all the recommendations, the service provider computes T_{recom} using each recommendation received (T_i) as:

$$T_{recom} = \begin{cases} Undefined & if\ i = 0 \\ \frac{\sum_{i=1}^{n} T_i}{n} & if\ i > 0 \end{cases}$$

Where i denotes number of recommenders. According to equation, if the recommendation requestor receives no recommendation for the target service, i.e, i = 0 the recommended trust value T_{recom} is set to be undefined. This usually happens when the service requestor is a new service and has no previous interaction with any other services in the environment.

4.2.6 Thresholds for Collusion Detection

Two values for possible collusive behavior:

(1) After the calculation of all the DF & SF, if there is a slight/ small discrepancy in the recommendations received; then the nodes will be ***doubtfully*** in collusion and we will decrement their trust values T_i. These recommendations won't take part in Trust calculation.

(2) If the discrepancy is wide/ broad (almost opposite) to other nodes then they will be ***definitely*** in collusion and will be added to 'distrusted'.

If nodes give a trust value which is opposite of the majority: i.e.

- **Badmouthing attack**: If node gives false malicious value for a trusted node then the nodes with the malicious values are colluding (colluding group) and want to decrease the trustworthiness (reputation) of a trusted node.
- **Ballot stuffing attack**: If the false recommendations which cause the trust value of the malicious node to increase – then the target node and the nodes giving false values will be in definite collusion by launching ballot stuffing attack.

Note: Trust values will be decremented by a value of (0.1). Nodes distrusted 3 times will be blacklisted.

4.2.7 History

Since trust values for other nodes change; node n_i maintains a partial history of interactions with other nodes declared as $Hi = \{Direct / Indirect, n_j, \alpha, b, T_{i,j}, ttl\}$

where *Direct/ Indirect* means that the value is from direct interaction or from other reference/ witness nodes, n_j is the target node, α and β are constant or dynamic values (increment in case of cooperation and decrement in case of defection), $T_{i,\,j}$ is trust value of node n_j in the range *[0, 1]*, *ttl* is the time stamp when the trust value is determined. Older values from the history database are discarded based on ttl value.

4.3 Conclusion

In this chapter the details of proposed collusion resistant Sybil attack detection scheme is discussed. The proposed scheme achieves all the Sybil and Collusion detection goals, considered while designing the proposed scheme. The proposed method is designed to calculate trustworthiness of every node, examine the behavior pattern of nodes, detect, and thwart collusion and Sybil attacks. Instead of designated nodes, each mobile node in the network monitors packets passing through it and exchanges its observations in order to determine Sybil attack. Malicious nodes producing false recommendations are detected and made ineffective. In short, the evaluator node in this scheme utilizes a multi-dimensional trust model to detect Sybil attacks with 100% accuracy and also detect and prevent collusion of malicious nodes. The proposed scheme claims that it effectively encounters all the weaknesses and vulnerabilities present in the previous schemes.

Chapter 5

PERFORMANCE EVUALATION/ EMPIRICAL EXPERIMENTS

5.1 Introduction

This chapter provides an experimental evaluation of the Collusion Resistant Sybil attack detection model proposed in the previous chapter. Several experiments are proposed and conducted. These experiments are designed and conducted for three reasons: (1) demonstrating the vulnerability of existing Sybil attack detection models against individual-level attacks like collusion attack (2) empirically showing the necessity of the requirements proposed in chapter 4 for Sybil attack detection in the presence of collusion and (3) demonstrating how the proposed trust model is resistant against the collusion attack (the witness-based collusion attack).

The implementation of any proposed protocol or scheme expresses the applicability of that proposed scheme. Two approaches are primarily adopted to demonstrate the working of any scheme or protocol. The first approach is to simulate that protocol by using simulator like NS-2, OMNet++ etc. The results achieved by these simulators are consider reliable and are widely acceptable in research communities. The second approach is to implement the proposed protocol and experiment the proposed protocol on actual network architecture.

In this chapter, the strength of proposed scheme as compared to previous Sybil attack detection scheme is described and proved. As discussed in chapter 3, the previous Sybil attack detection schemes are fail to detect Sybil nodes accurately in the presence of Collusion attack. The computational cost and the communication cost of proposed scheme is compared with the existing Sybil attack detection schemes. The simulation is tested using different test vectors of varied input and the results are analyzed.

5.2 Experimentally Evaluated Policies

This section describes policies used by experimentally evaluated node types.

5.2.1 Direct Interaction Policies

Two kinds of Direct Interaction Policies are used in our experiments are: Always Cooperate (AC), Always-Defective (AD). Always Cooperate and Always Defect have been called unconditional cooperation and unconditional defection respectively. Nodes using the AC policy for their direct interactions will cooperate with their neighbors in direct interactions regardless of the action of their neighbor. In contrast, nodes using the AD policy will defect in all neighbor interactions.

5.2.2 Witness Interaction Policies

Answering policy (AP) is mainly used in our experiments as Witness Interaction Policy. Three sub types of answering policies in our experiments: Honest (Ho), Liar (Li), and Simpleton (Si). The Honest policy always tells the truth to everyone. An node employing the Liar policy gives manipulated ratings to other nodes by giving high ratings for untrustworthy nodes and low ratings for trustworthy ones. The Simpleton policy always ranks all other nodes as trustworthy. In this sense, Liar always defects, Honest always cooperates, and Simpleton sometimes defects (by providing a high rating for untrustworthy nodes) and sometimes cooperates (by providing a low rating for trustworthy nodes) in providing the witness information.

5.3 Simulation Parameters and Metrics

5.3.1 Simulation Parameters

In order to implement and evaluate our scheme, we use Network Simulator NS-2.30 using the parameters listed in Table 1. The **UB_THRESHOLD** is the averaged received signal strength value (in Watts) of several scenarios when a transmitter is moving with 10 m/s speed; lower speeds thresholds will improve detection accuracy. The **TIME_THRESHOLD** is the average (maximum) time in which a node should listen from another node, otherwise that identity will be considered as out of range or previous identity of a whitewasher. Shorter time intervals will increase identity revalidations in the network; whereas lengthy intervals will increase table sizes in network nodes. We used 5 as an arbitrary number of records per identity; however, it can be increased depending upon the memory capacity of nodes.

In this simulation study our aim is to establish the detection percentage of our proposed scheme in different scenarios. As we discussed above, there are some attributes of the network that are mainly responsible for affecting the accuracy of our Collusion Resistant Sybil attack detection scheme. These attributes are number of network connections, node density and transmission rate. In each of our scenario we take speed as our main attribute. All of the results we present here have been calculated as an average of 15 different random scenarios (or simulation runs).

Table 1 Simulation Parameters

Parameter	Level
Area	1000m × 1000m
Speed	8 to 12 m/s
Pause Time	10 to 20 s
Radio Propagation Model	Two-ray Ground Reflection
Radio Range	250m
Carrier Sense Range	550m
Number of Nodes	30 to 40
MAC	802.11
Simulation Time	300 s
Mobility Model	Random Waypoint Model
Malicious Population	25%
Sybil Ids per Malicious Node	5
UB_RSS_THRESHOLD	6.45×10^{-10} Watts
Interaction Type	Direct & Indirect
Trust Value	[0,1]

5.3.2 Metrics

We use four main metrics in order to determine the detection accuracy of our scheme in different environments, i.e. Collusion detection percentage, Sybil node detection percentage, True Positive Rate (TPR) and False Positive Rate (FPR). True positive means a malicious node is correctly detected and false positive means a good or legitimate node is incorrectly detected as a malicious one, as given below.

$$True\ Positive\ Rate = \frac{Correctly\ Detected\ Sybil\ IDs}{Total\ Sybil\ IDs}$$

$$False\ Positive\ Rate = \frac{Incorrectly\ Detected\ Benign\ IDs}{Total\ Benign\ IDs}$$

$$Collusion\ Detection\ Rate = \frac{Correctly\ Detected\ Colluded\ IDs}{Total\ Colluded\ IDs}$$

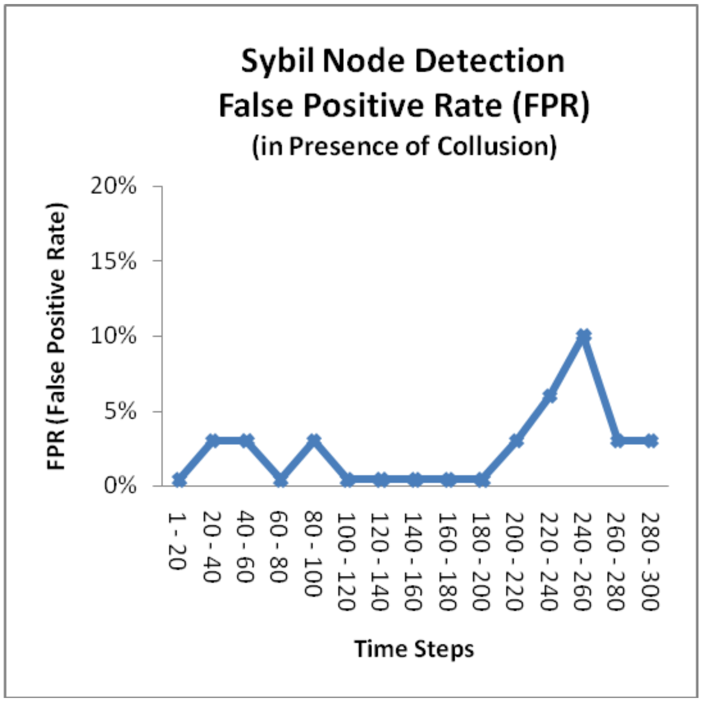
$$Sybil\ Detection\ Rate = \frac{Correctly\ Detected\ Sybil\ IDs}{Total\ Sybil\ IDs}$$

5.4 Analysis

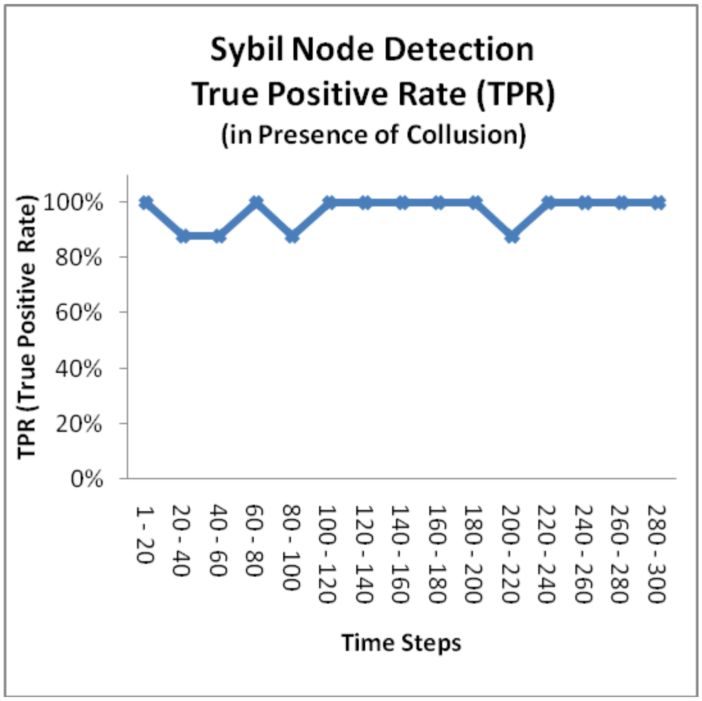
In this section we will analyze our scheme for the detection of Sybil and collusion attacks and the True Positive and False Positive Rates of the detection.

5.4.1 Sybil Attack Detection

As shown in Graph 1, our scheme detects Sybil nodes very efficiently and accurately in the presence of malicious colluding nodes. False positives remained below 5% level, as depicted in Graph 1. Node density in the network is inversely proportional to the false positives of our scheme. For detection, movement sensing or the reception of frequent RSS values are important. In order to obtain RSS values from a node, that node should be involved in some form of communication, for example by acting as a source, forwarder, or destination. The more frequently a node sends or receives packets, the more efficiently a neighboring node will detect it in the event that it tries to create its Sybil identity. Fewer connections in a network imply fewer source and destination nodes, and greater difficulty for a node to distinguish other nodes' positions. Consequently a greater number of false positives will result. However, connections have no apparent effect on the true positives and for most of our experiments the true positives remained around the 90% level, as depicted in Graph 2.



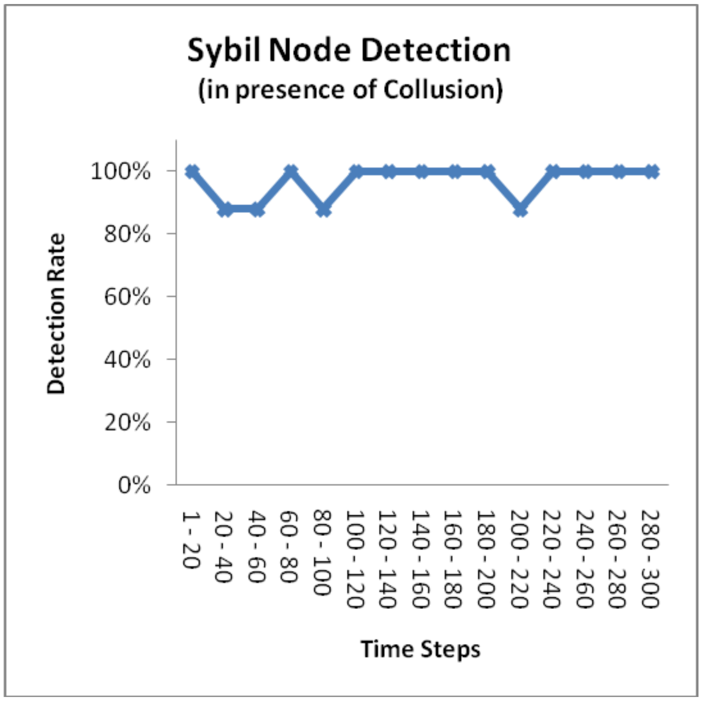
Graph 1

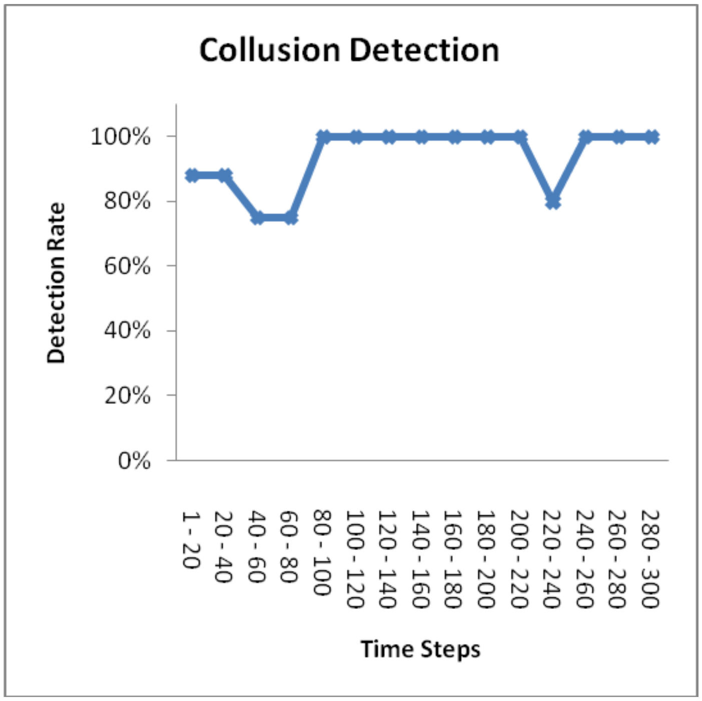


Graph 2

5.4.2 Collusion Attack Detection

Graph 3 shows the Sybil Node detection rate. The network diagram is for 300 time steps. Collusion resistant/prevention/ detection method defined in Section C is applied, because malicious nodes can maintain connections with benign nodes and collaborate to decrease the detection rate and overall performance of the network. However the Figure shows very efficient detection rate of Sybil nodes (TPR), it can be seen that the Collusion resistant/prevention/ detection method works very well in the network for the detection of Sybil nodes accurately. The overall Sybil detection rate is above 90% level. In Graph 4, the Collusion detection rate of our scheme is shown on the basis of Collusion resistant/prevention/ detection method defined in Section C. Again the Figure shows very efficient detection rate of Colluded nodes, i.e. almost 90%. This shows that the policies defined for detection of Colluded nodes are effective in reducing the risky collaboration among malicious nodes and benign nodes and promoting a malicious node or defaming a benign node, thus preventing the collusion attack.

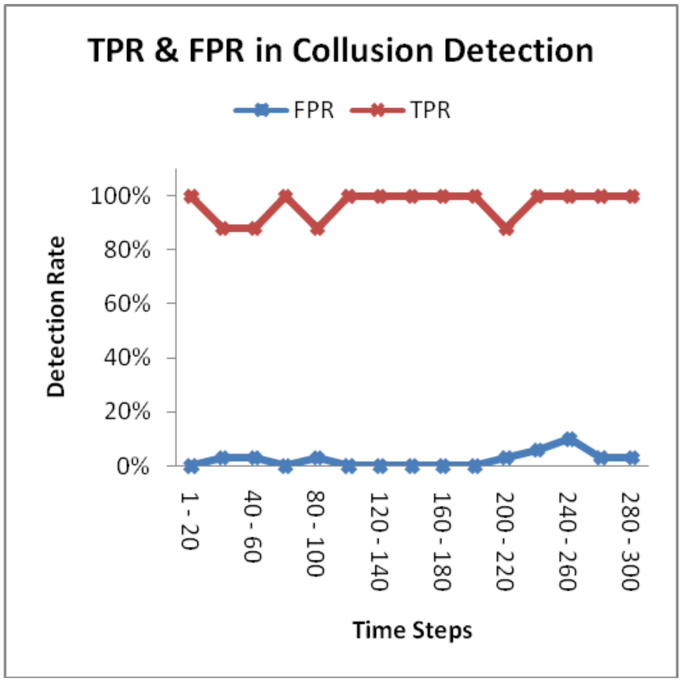




Graph 3

Graph 4

The final Graph 5, as shown, our scheme detects colluded nodes very efficiently. Node density in the network is inversely proportional to the false positives of our scheme. The figure shows the True Positive and False Positive detection rates of Colluded nodes. And as depicted in Graph 5, our experiments shows true positives remained around the 95% level and false positives around 10% level. This shows that our scheme work better in MANET environments where nodes where one or more users conspire together to take advantage of breaches in trust models to defraud one or more users. The results show that our scheme overcomes the collusion problem to a great extent.



Graph 5

From the above analysis it is evident that our scheme work better in MANET environments where there are 25 to 40% malicious nodes, high network connections, node density, and packet transmission rate. The detection accuracy will be improved when nodes move with low speeds. In the simulation it should be less than 10m/s and in real-world scenarios at most 2m/s. The objective of these experiments is to demonstrate the benefit of using a multi-dimensional model when there are direct and witness based collusion attacks. Using the witness interaction trust and witness based reputation can decrease the impact of malicious nodes (colluding groups) on aggregating the ratings.

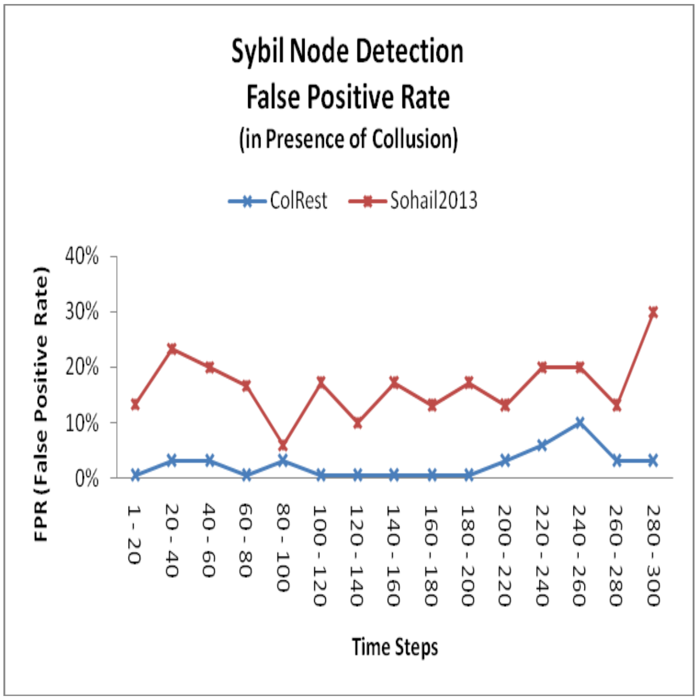
5.5 Comparison with other Sybil detection Schemes

Here we will explain our conducted experiments and corresponding results of the Collusion attack on Sybil attack detection against an existing well-known Sybil detection model and our proposed collusion-resistant Sybil detection model in Mobile ad-hoc networks. We have selected Abbas et al. [7] as the representative of the existing well-known Sybil detection model in MANETs with the supposed name of ‘**Sohail2013**’.

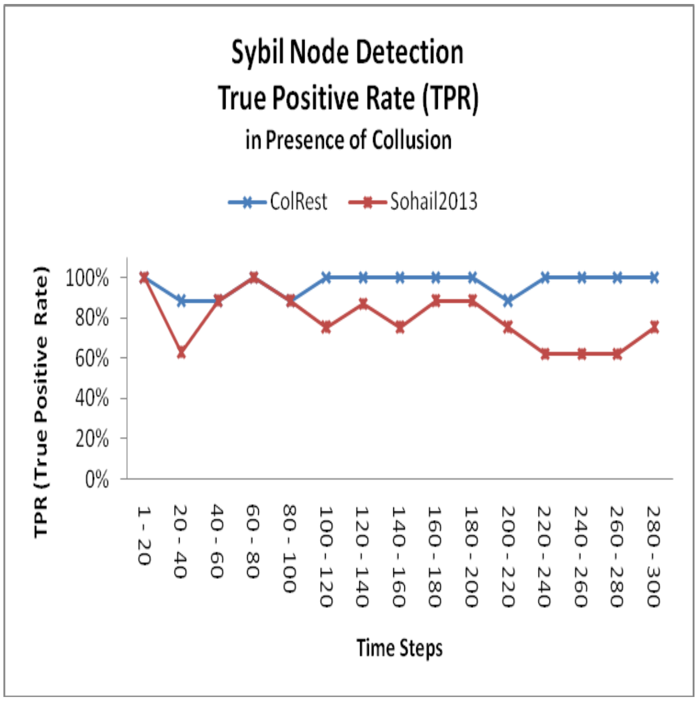
All simulations graphed in this section were run with and without Collusion resistant model for Sybil attack detection. **Sohail2013** assumed that there will be no collusion and the nodes will cooperate with each other and will be trusted. On the other hand "**ColRest**" will accurately detect Sybil attacks in the presence of collusion and also detects and prevents from collusion attacks.

5.5.1 Results and Discussions

As shown in Graph 6, our scheme detects Sybil attack very efficiently in the presence of collusion attack with very low False Positive Rate (FPR). Node density in the network is inversely proportional to the false positives of our scheme. For detection, movement sensing or the reception of frequent RSS values are important. In order to obtain RSS values from a node, that node should be involved in some form of communication, for example by acting as a source, forwarder, or destination. The more frequently a node sends or receives packets, the more efficiently a neighboring node will detect it in the event that it tries to create its Sybil identity. Fewer connections in a network imply fewer source and destination nodes, and greater difficulty for a node to distinguish other nodes' positions. Consequently a greater number of false positives will result. However, connections have no apparent effect on the true positives and for most of our experiments the true positives remained around the 90% level, as depicted in Graph 7. And on the contrary the True Positive Rate of **Sohail2013** is much low than **ColRest** in the present of collusion. Means our scheme detects Sybil attack in a very accurate and efficient manner.

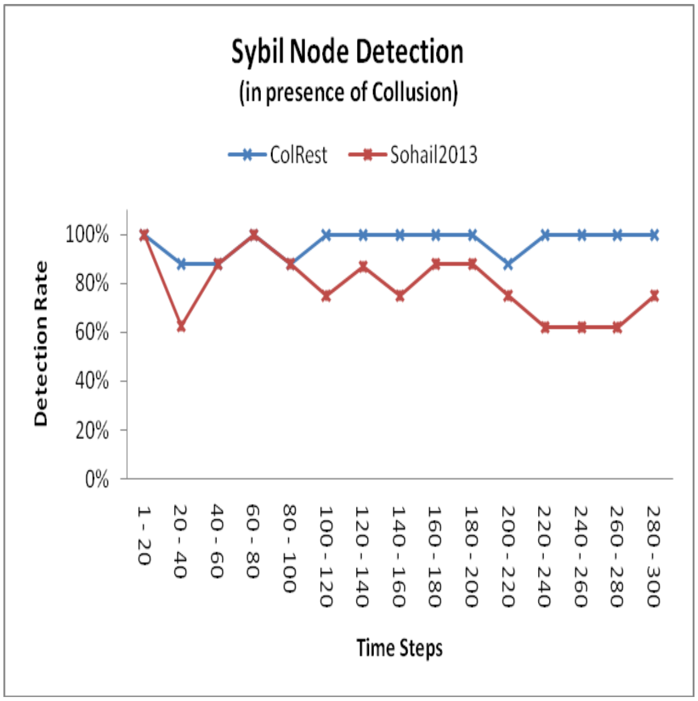


Graph 6

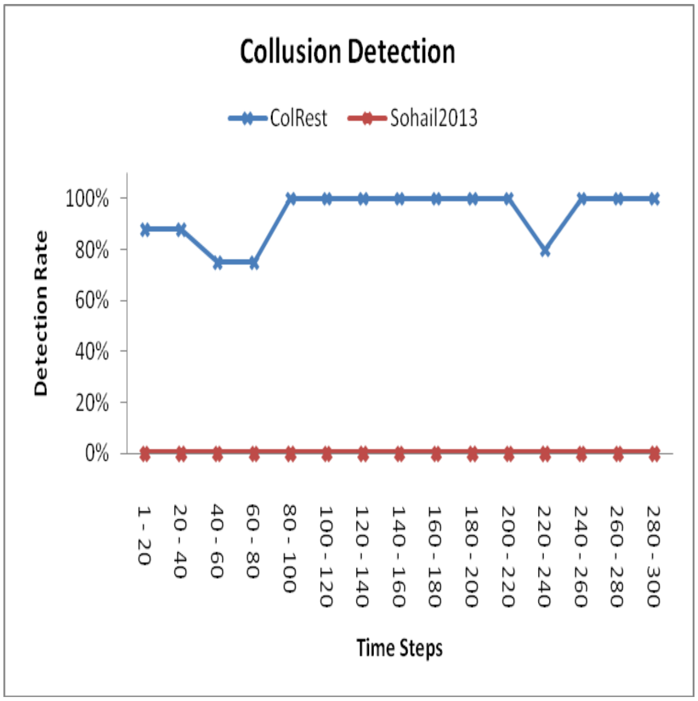


Graph 7

Graph 8 shows the Sybil Node detection rate. The network diagram is for 300 time steps. Collusion resistant/prevention/ detection method defined in Section C is applied, because malicious nodes can maintain connections with benign nodes and collaborate to decrease the detection rate and overall performance of the network. However the Figure shows very efficient detection rate of Sybil nodes (TPR), it can be seen that the Collusion resistant/prevention/ detection method works very well in the network for the detection of Sybil nodes accurately as compared to **Sohail2013** where the graph is much lower than the ColRest. In Graph 9 the Collusion detection rate of our scheme on the basis of Collusion resistant/prevention/ detection method defined in Section C. Again the Figure shows very efficient detection rate of Colluded nodes. This shows that the policies defined for detection of Colluded nodes are effective in reducing the risky collaboration among malicious nodes and benign nodes and promoting a malicious node or defaming a benign node, thus preventing the collusion attack. On the other hand the very best feature of our scheme as compared to **Sohail2013** is that; **Sohail2013** only detects Sybil attack (assumed there will be no collusion) while our scheme ColRest not only detect Sybil attack in the presence of collusion attack and also detects colluding nodes and isolates it from the network.



Graph 8



Graph 9

The above figures shows that our scheme work better in MANET environments where one or more users conspire together to take advantage of breaches in trust models to defraud one or more users. The results show that our scheme overcomes the collusion problem to a great extent.

5.6 Conclusion

The proposed Collusion resistant Sybil attack detection scheme is implemented and simulated using Network Simulator NS-2.30 using the parameters listed in Table 1. The security of the proposed scheme is analyzed by considering various attack scenarios. The strength of the proposed scheme against these attack scenarios is examined. The security analysis proved that all the weaknesses and vulnerabilities reside in previous schemes has been encountered effectively, i.e. our scheme detects Sybil attack very efficiently in the presence of collusion attack with very low False Positive Rate (FPR).

The above figures shows that our scheme works better in MANET environment where one or more users conspire together to take advantage of breaches in trust models to defraud one or more users. The results show that our scheme overcomes the collusion problem in Sybil attack detection process to a great extent.

Chapter 6

CONCLUSION

6.1 Overview

This thesis is motivated by the dire need for collusion resistant Sybil attack detection model in MANETs by employing multi-dimensional trust model (trust is based on direct as well as indirect interactions) in open and distributed environments, especially disconnected MANETs. While surveying important existing Sybil attack detection models from the literature as showed in Chapter 3, through localization and RSSI, we have noted a tendency to focus on exploitation of these localization models while detection Sybil nodes. As a result, we have noted the exposure of such models to collusion attacks. These vulnerabilities reinforce the need for new evaluation criteria for Sybil attack detection in the presence of selfish and malicious colluded nodes called ‘Collusion resistant Sybil attack detection’ which reflects the ability of a detection model to be unaffected by conspiring nodes who try to manipulate the recommendations or providing false recommendations in the detection model.

We have proposed a decentralized multi-dimensional trust model. The proposed model is compatible with the characteristics of open and distributed MANETs. The proposed 'Collusion Resistant Sybil Attack detection' model provides the facility to define nodes with various behaviors and is flexible enough to accommodate a variety of adversarial behaviors. The proposed scheme does not suffer from the shortcomings of existing Sybil detection schemes, like the assumption that there will be no collusion among malicious nodes, nodes will be cooperative and network will be static with no mobility considered. The simulation results demonstrated that our proposed schemes worked better in discouraging and detecting these attackers while maintaining good network performance.

We show the vulnerability of uni-dimensional trust models, i.e. trust only based on direct interactions, against collusion attacks while detecting Sybil attacks. We proposed strategies for dealing with witness-based collusion attacks. We found that when detection Sybil attacks in colluded environments, trust models need to be multi-dimensional in order to be resistant against collusion attacks. Moreover, we show that trust-aware nodes needs multi-dimensional trust models to separate malicious and naive nodes from the trustworthy community.

Our scheme detects Sybil attack very efficiently in the presence of collusion attack with very low False Positive Rate (FPR). This shows that the policies defined for detection of Colluded nodes are effective in reducing the risky collaboration among malicious nodes and benign nodes and promoting a malicious node or defaming a benign node, thus preventing the collusion attack in the detection of Sybil attacks. Our scheme works better in MANET environments where one or more users conspire together to take advantage of breaches in trust models to defraud one or more users. The results show that our scheme overcomes the collusion problem to a great extent. Through the help of extensive simulations and experiments, we are able to demonstrate that our proposed solution detects Sybil or whitewashers' new identities with good accuracy and reduces the benefits of collusion even in the presence of mobility.

The security analysis of the proposed scheme verified that all the weaknesses and vulnerabilities present in the existing Sybil attack detection schemes are effectively encountered. The proposed Collusion Resistant Sybil attack detection scheme fulfills all the requirements that any Collusion Resistant Sybil attack detection scheme for wireless networks should posses.

6.2 Future Work

The Collusion resistant Sybil attack detection is of paramount importance for wireless communication networks. This thesis addressed many security vulnerabilities of existing schemes of Sybil attack detection. In future the proposed scheme will be extended to a more robust and efficient scheme for the detection and prevention of richer and more varied attacks that attempt to exploit one or more information sources and proposing solutions for them. We will enhance our scheme to make it feasible in pervasive computing environment and E-Commerce societies.

BIBLIOGRAPHY

[1] S. A. Razak, S. M. Furnell and P. J. Brooke. Attacks against Mobile Ad Hoc Networks Routing Protocols. In Proceedings of 5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting, PGNET 2004, 2004.

[2] J. Merwe, D. Dawoud, and S. McDonald, "A survey on peer-to-peer key management for mobile ad hoc networks," ACM Computing Surveys, vol. 39, p. 1, 2007.

[3] J. R. Douceur, "The Sybil Attack," in Revised Papers from the First International Workshop on Peer-to-Peer Systems: Springer-Verlag, 2002.

[4] M. Srivatsa, "Who is Listening? Security in Wireless Networks," in International Conference on Signal Processing, Communications and Networking, ICSCN India, 2008, pp. 167-172.

[5] Iltaf et al.: A mechanism for detecting dishonest recommendation in indirect trust computation. EURASIP Journal on Wireless Communications and Networking 2013 2013:189

[6] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack In Sensor Networks: Analysis & Defences," in Third International Symposium on Information Processing in Sensor Networks (IPSN'04) 2004, pp. 259-268.

[7] S. Abbas, M. Merabti, and D.Llewellyn-Jones, "A Lightweight Sybil Attack Detection in MANETs," IEEE Systems Journal, 2012

[8] T. Suen and A. Yasinsac, "Ad hoc network security: peer identification and authentication using signal properties," in Proceedings of the Sixth Annual IEEE SMC Information Assurance Workshop (IAW '05) New York, 2005, pp. 432-433.

[9] Z. Li, W. Trappe, Y. Zhang, and B. Nath, “Robust statistical methods for securing wireless localization in sensor networks,” in Proc. 4th Int. Symp. Information Processing in Sensor Networks, 2005, pp. 91–98.

[10] Niraj et. al. Distributed Position Localization and Tracking (DPLT) of Malicious Nodes in Cluster Based Mobile Ad hoc Networks (MANET), WSEAS

Transactions on Communications, ISSN: 1109-2742, Issue 11, Volume 9, November 2010

[11] F. Mourad, H. Snoussi, and C. Richard, “Interval-Based Localization using RSSI Comparison in MANETs,” IEEE Transactions on Aerospace and Electronic System, vol. 47, pp. 2897–2910, 2011

[12] S. Abbas, M. Merabti, and D.Llewellyn-Jones "Signal Strength Based Sybil Attack Detection in Wireless Ad Hoc Networks" (2009) Second International Conference on Developments in eSystems Engineering (DESE), UAE

[13] J. Li, R. Li, and J. Kato, “Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks,” IEEE Comm. Mag., Vol. 46, No. 4, April, pp. 108-114, 2008.

[14] Lian, Q., Zhang, Z., Yang, M., Zhao, B.Y., Dai, Y., Li, X.: An empirical study of collusion behavior in the Maze P2P file-sharing system. In: Proceedings of the 27th (ICDCS 2007), pp.56, 2007.

[15] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack In Sensor Networks: Analysis & Defences," in Third International Symposium on Information Processing in Sensor Networks (IPSN'04) 2004, pp. 259-268.

[16] Z. Sheng, L. Li, L. Yanbin, and Y. Richard, "Privacy-Preserving Location based Services for Mobile Users in Wireless Networks," Department of Computer Science, Yale University, Technical Report ALEU/DCS/TR-1297, 2004.

[17] M. Demirbas and Y. Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," in Proceedings of the International Symposium on World of Wireless, Mobile and Multimedia Networks: IEEE Computer Society, 2006.

[18] J. Wang, G. Yang, Y. Sun, and S. Chen, "Sybil Attack Detection Based on RSSI for Wireless Sensor Network," in International Conference on Wireless Communications, Networking and Mobile Computing (WiCom'07), 2007, pp. 2684-2687

[19] L. Shaohe, W. F. Xiaodong, Z. Xin, and Z. Xingming, "Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks," in International Conference on Computational Intelligence and Security, CIS '08. vol. 1, 2008, pp. 442-446.

[20] T. Suen and A. Yasinsac, "Ad hoc network security: peer identification and authentication using signal properties," in Proceedings of the Sixth Annual IEEE SMC Information Assurance Workshop (IAW '05) New York, 2005, pp. 432-433.

[21] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In Proceedings of IEEE INFOCOM ’05, 2005.

[22] B. Xiao, B. Yu, and C. Gao, "Detection and Localization of Sybil Nodes in VANETs," in Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks Los Angeles, CA, USA: ACM, 2006.

[23] M. Talasila, R. Curtmola, and C. Borcea, "LINK: Location-verification through immediate neighbors knowledge," Department of Computer Science, NJIT, Tech.Rep., 2010.

[24] Liu, D., Ning, P., and Du, W. K. 2005. Attack-resistant location estimation in sensor networks. In Proceedings of the 4th international Symposium on information Processing in Sensor Networks (IPSN) (Los Angeles, California, April 24 - 27, 2005).

[25] Y. Hao, J. Tang, and Y. Cheng, "Cooperative Sybil attack detection for position based applications in privacy preserved VANETs", in Proc. IEEE GLOBECOM, Houston, Texas, Dec. 5-9, 2011

[26] A. Salehi-Abari and T. White, “Towards con-resistant trust models for distributed node systems,” in IJCAI ’09: Proceedings of the 21 International Joint Conference on Artificial Intelligence, 2009.

[27] Huynh, T.D., Jennings, N.R., Shadbolt, N.: FIRE: An integrated trust and reputation model for open multi-node systems. Journal of Autonomous Nodes and Multi-Node Systems Vol. 13, No. 2, pp. 119–154, 2006

[28] B. Yu and M. P. Singh, “A social mechanism of reputation management in electronic communities,” in CIA ’00: Proc of the 4th Intl. Workshop on Cooperative Information Nodes IV, Springer-Verlag, pp. 154–165, 2000

[29] A Arning, R Agrawal, P Raghavan, A linear method for deviation detection in large databases, in 2nd International Conference on DataMining and Knowledge Discovery (AAAI, Portland, 1996), pp. 164–169

[30] Jarvenpaa, S.L., Tractinsky, N., Vitale, M.: Consumer trust in an internet store. Inf. Technol. and Management 1(1-2), 45–71 (2000)

[31] Amirali, S.-A., Tony, W.: Witness-based collusion and trust-aware societies. In: SPOSN 2009: the Workshop on Security and Privacy in Online Social Networking (2009)

[32] Djenouri, D., Khelladi, L., et al., "A Survey of Security Issues in Mobile Ad hoc and Sensor Networks," IEEE Communications Surveys & Tutorials, vol. 7, pp. 2,28, 2005.

[33] U. Banerjee and A. Swaminathan, "Taxonomy of Attacks and Attackers in MANETs," International Journal of Research and Reviews in Computer Science (IJRRCS), vol. 2 pp. 437,442, April 2011.

[34] R. Sheikh, M. S. Chandel, and D. K. Mishra, "Security Issues in MANET: A review," in Seventh International Conference On Wireless And Optical Communications Networks (WOCN) 2010, pp. 1,4.

[35] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: the dynamic source routing protocol for multihop wireless ad hoc networks," in Ad hoc networking (Ch 5), ed: Addison, Wesley Longman Publishing Co., 2001, pp. 139,172.

[36] C. E. Perkins and E. M. Royer, "Ad,hoc on,demand distance vector routing," presented at the Second IEEE Workshop on Mobile Computing Systems and Applications, WMCSA 1999.

[37] C. E. Perkins and P. Bhagwat, "Highly dynamic Destination,Sequenced Distance, Vector routing (DSDV) for mobile computers," SIGCOMM Computer Communication Review, vol. 24, pp. 234,244, 1994.

[38] Y. Yoo, S. Ahn, and D. P. Agrawal, "A credit,payment scheme for packet forwarding fairness in mobile ad hoc networks," presented at the IEEE International Conference on Communications (ICC), 2005.

[39] Y. Yoo and D. P. Agrawal, "Why does it pay to be selfish in a MANET?," Wireless Communications, IEEE, vol. 13, pp. 87,97, 2006.

[40] K. Mandalas, D. Flitzanis, G. F. Marias, and P. Georgiadis, "A survey of several cooperation enforcement schemes for MANETs," presented at the Proceedings of

the Fifth IEEE International Symposium on Signal Processing and Information Technology 2005.

[41] Whitby, A., Jsang, A., Indulska, J.: Filtering out unfair ratings in bayesian reputation systems. In: Proceedings of 7th International Workshop on Trust in Node Societies (2004)

[42] B. N. Levine, C. Shields, and N. B. Margolin, "A Survey of Solutions to the Sybil Attack," Technical Report 2006-052, University of Massachusetts Amherst, Amherst, MAOctober 2006.

[43] V. A. Luis, B. Manuel, and L. John, "CAPTCHA: Using Hard AI Problems For Security," presented at the Proceedings of Eurocrypt, 2003.

[44] S. Abbas, M. Merabti, and D. Llewellyn-Jones, "Deterring Whitewashing Attacks in Reputation based Schemes for Mobile Ad hoc Networks," in Wireless Days (WD), IFIP, 2010, pp. 1-6.