ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

Smart Duo Approach - Detection and Removal of Sybil attackers in MANETs by Clump based Scheme

Mr. Suresh N, Mrs. Madhuri T

Student 2nd Year MTech, Dept. of ISE, The Oxford College of Engineering, Bangalore, Karnataka, India.

Assistant Professor, Dept. of ISE, The Oxford College of Engineering, Bangalore, Karnataka, India.

ABSTRACT - It is quite a challenging task to achieve security in Mobile ad hoc networks (MANETs) because of its open nature, high mobility of nodes, lack of infrastructure and central management. Sybil attackers as enters into the network they start to create multiple identities, by this each created identities also takes part in disrupting the network by participating in communication with legitimate nodes. This cause's huge loss in network resources and this type of attacks are difficult to detect and control so quickly. So this makes a way for several researchers to design security based approaches to mitigate these problems. In this paper, first we focus on the issue to enhance the accuracy of Detection[2] process by Comparing threshold values as well as Node IP address and Certificate revocation[8][9] to cut off attackers from network so that attackers can be stopped from further participating in the network.

KEYWORDS - Certificate Revocation, IP, Mobile Ad Hoc Networks (MANETS), Network Security, RSS, Threshold, and Sybil Attack

I. INTRODUCTION

A **mobile ad hoc network** (**MANET**) is a self-configuring infrastructure less network of mobile devices connected by wireless. The MANET topology is dynamic in nature due to the constant movement of nodes to communicate each other to share resources, so in a MANET each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great features also come with serious drawbacks from a security point of view. Security [6] is one of the essential requirements for mobile ad hoc network services to save resources and freeing the network from attackers. Characteristics of MANETs such as Distributed nature, Availability, Authentication, Confidentiality, Access control, and Integrity are the challenging one's to safeguard the MANETs. Implementing security methods in such networks is therefore of most important to secure network from attackers.

Due to infrastructure less feature of MANETs, every nodes in the network themselves participate in implementing the every aspect related to network functionalities where nodes acts as both users and routers, which transfers packets to other nodes and another feature of MANETs is the open network environment where nodes can join and leave the network freely which is provides a flower path for attackers to participate in network to cause disruption in resource sharing, therefore dynamic natures of MANETs is more vulnerable to various types of attacks than the wired networks.

In this paper, we show that the mobility of nodes in a mobile ad hoc network can be used to detect and identify nodes that are part of a Sybil attack and process of certification revocation by neighboring nodes [5].

In the first method called Detection, our designed approach utilizes the RSS [3] [4] and IP or MAC which differentiates the legitimate node and Sybil nodes while every node entering into the radio range of the neighboring [5] nodes. Usually in MANETs nodes enters into the network and exits after the task based on this we define a threshold which differentiates legitimate node and Sybil node, in this we compare RSS of the entered node with the default threshold. Second through IP or MAC Comparison, a single node can detect Sybil attacks by recording the identities, namely the MAC or IP addresses of other nodes it hears transmitting. Over time, the node builds a profile of which nodes are heard together, which helps reveal Sybil attackers?

In the second method so called Revocation process, among all security based issues in mobile ad hoc networks, the most widely used mechanism is so called certificate management which helps in invalidation of Sybil identities can be done to secure network. Certificate management to invalidate certificate encompasses two components which are detection and revocation. Certification Invalidation is a necessary to secure network communications. It is designed in such a way that communications between nodes in the network and Certification authority, who actually responsible for sharing and storing valid certificates. Certificate Revocation is the task of removing the certificates of nodes that have been detected as attackers by the neighborhood nodes. We can say in other way as, if a parent Sybil node creates multiple identities to compromise the MANET, those nodes should be cut off from the network so that they can be stopped from further participating in the network. In our proposed approach, we focus on the both detection and removing of Sybil nodes from the network to secure the MANETs from several threats.

The remaining of the paper is organized as follows. Section 2 highlights the problem statement. In Section 3, we surveyed some papers on MANETs and put in related work. In Section 4, we described our proposed approach. This paper is concluded in Section 5.

II. PROBLEM STATEMENT

Sybil attack has caused too much threaten to Mobile ad hoc network in routing, voting system, fair resource allocation, data aggregation and misbehavior detection. To mitigate these issues several research works have been taken out from many researchers.

III. RELATED WORK

Many research works have investigated the problem of malicious node detection in MANETs. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost for detecting cooperative Sybil attacks.

Demirbas and Song proposed Received Signal Strength Indicator (RSSI) based solution to detect the Sybil attack in the wireless sensor networks. It is based on the fact that a malicious node with a number of fake IDs will have the same signal strength. They showed that even though RSSI is time varying and unreliable in general and radio transmission is non-isotropic; using the ratio of RSSIs from multiple receivers it is feasible to overcome these problems. The malicious node can vary its transmission power for its Sybil node leading to different received signal strength and hence inaccurate detection of Sybil identities. This approach is not suitable for the MANETs, if the nodes move with non-uniform speeds

Piro et al. used the mobility of nodes as a feature to detect the Sybil attack in MANETs. This mechanism is based on the fact that all the Sybil nodes of a malicious node will always move together. If a set of nodes are seen together for a long period of time by an observer node, then they are suspected to be the identities of Sybil attacker. The accuracy of the detection mechanism can be further improved by using multiple trusted observer nodes. However, this scheme fails if the malicious node continuously changes the identities of its Sybil nodes.

D. Monica, J. Leitao, L. Rodrigues, and C. Ribeiro proposed Resource testing scheme in this approach, various tasks are distributed to all identities of the network in order to test the resources of each node and to determine whether each independent node has sufficient resources to accomplish these tasks. These tests are carried out to check the computational ability, storage ability and network bandwidth of a node. A Sybil attack will not possess a sufficient amount of resources to perform the additional tests imposed on each Sybil identity. The drawback of this approach is that an attacker can get enough hardware resources, such as storage, memory, and network cards to accomplish these tasks.

H. Liming, L. Xiehua, Y. Shutang, and L. Songnian proposed security scheme called "Fast authentication public key infrastructure for mobile ad hoc networks based on trusted computing," This is a one-to-one mapping of a hardware device and a network entity. In other words, one hardware device, such as network card is bound to a single network entity. However, there is no way of preventing an entity from obtaining multiple hardware devices, for example in a scenario in which an attacker installs two network cards. Capkun *in* "Mobility helps peer-to-peer security" exploited mobility to enhance security in MANETs. A MANETs which is self organized, where there is no central authority, nodes establish security associations purely by mutual agreement. Users can activate a point-to point secure side channel (SSC) using infrared or wired media between their personal devices to authenticate each other and set up shared keys when they are in close proximity to each other. The author attempts to solve the problem of impersonation and Sybil attacks by binding a user's face and identity using these SSCs. However, SSCs are based on the assumption that nodes are connected through wired or infrared connections.

C. Piro, C. Shields, and B. N. Levine, "Detecting the Sybil attack in mobile ad hoc networks, "proposed to detect Sybil identities by observing node dynamics. Nodes are keeping track of identities which are often seen together (Sybil identities) as opposed to the honest distinct nodes that move freely in different directions. However, the scheme will produce high false positives where node density is high, such as a conference hall or nodes moves in a same direction, such as a group of soldier moving toward a target.

IV. PROPOSED APPROACH

In this paper we proposed a smart duo approach where detection and removal of malicious nodes can be easily carried in the appropriate way. Prior to detection scheme we are going to construct a clump [10] so that communication among each node will continuous by sending HELLO packet each other.

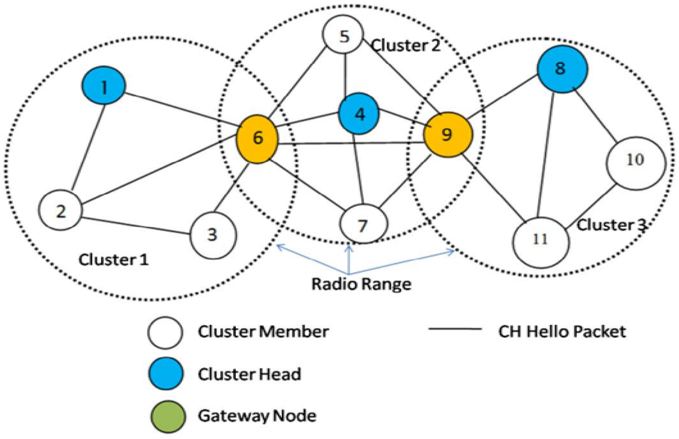

Fig.1 Clump Construction

In the next process we carry the IP Assignment scheme which can be viewed as handshaking protocol because both the agents i.e. Server node and Client node confirms each other by broadcasting ACK messages, Client node requests IP address as it enters into the network and Server nodes delivers and assigns the IP address.

Step 1. The client node periodically broadcasts messages to server nodes in the network using its hardware address (MAC).

Step 2. When a server node receives this broadcast message, it responds by sending a reply message using its IP address and the client's hardware address. It is possible that two or more servers reply to the same broadcast message.

Step 3. The client node sends an acknowledgment message back to the server node. If the client node has received more than one reply messages from different servers, it sends the acknowledgment message only to the 1st server and ignores the rest.

Step 4. When the server node receives this message, it realizes that it is ready to assign a new IP address to the requesting client node. If the server has multiple blocks of IP addresses, it assigns one of these blocks to the client node. Otherwise, it divides its set of available IP addresses into two disjoint subsets. It then sends one subset to the client node and keeps the other subset with itself. The server also sends its latest version of IP address table to the client.

Step 5. When the client receives this set of available IP addresses, it assigns itself the 1st IP address from this set and keeps the rest as its available set of IP addresses. It then sends a confirm message to the server indicating a successful configuration.

Step 6. When the server receives this confirm message, it terminates the IP assignment process.

Next in the detection scheme we are not using any other hardware like Antenna, GPS, etc. that's why we called it as smart duo approach. We first collect data like Received Signal Strength, which is compared with the default threshold value, as we know natural entry of the nodes in the neighbor nodes RSS will be too low, but attacker nodes RSS value will be high, by this data we will plot graph RSS vs. Time, the we lookout for the IP or MAC address of each node entering into the radio range, why we are choosing IP or MAC details because an attacker may spoof IP address, to meet 100% accuracy in detection we collect both RSS and IP.

In the second scheme we present the process of Removing of Sybil nodes by invalidating their certificates to protect network being attack. To Remove a Sybil attacker's certificate, we are to considering three stages: first is accusation, where neighboring legitimate node checks any malicious nodes, if found it casts a accusation message to Certification authority, In the verifying stage CA verifies the certificate of the accuser node, if its valid certificate then CA casts a message to all nodes in the network which says Invalidate the Certificate of Sybil nodes this is notifying stage.

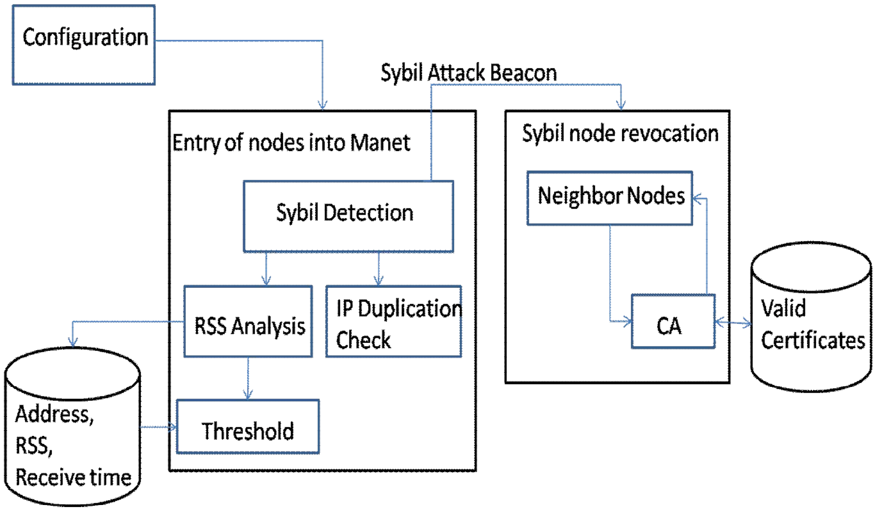

Fig.2 Proposed Architecture

V. SIMULATION AND RESULT

In order to implement and to check the effectiveness our scheme, we are using the necessary parameters listed in the below table 1. We considered the MANET environment within the 1000*1000m terrain area and the nodes in networks are deployed in the random uniform distribution with node speed limiting between 2 to 16m/s so that lower speeds improve detection accuracy. The *UB−THRESHOLD* is the averaged RSS value (in Watts) of several scenarios when a transmitter is moving with 10 m/s speed; 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; The *LIST−SIZE* is the maximum RSS records retained for an identity or address. We used 10 as an arbitrary number of records per identity; however, it can be increased depending upon the memory capacity of nodes.

In Fig 3 it reveals that as the node density in network increases it affects in the detection accuracy to conquer this issue we carried out two processes i.e. RSS comparison and IP spoof checking in detection scheme to meet up to 100% accuracy. In this fig when detection is true positive i.e. in the total no of Sybil identities how many malicious nodes correctly detected. In Fig 4 it shows the result when detection is false positive.

In Fig 5 it shows that how revocation is almost successful as though attacker nodes are more in the network. In the last fig it reveals the time taken in revocation process, as the no of attacker nodes are more there is slight increase in the time.

Parameters	Value
Mobility model	Random waypoint
Radio propagation model	Two-ray ground reflection
Terrain Area	1000m * 1000m
Node placement	Uniform distribution
Node speed	2 to 16 m/s
Radio range	250m
No of nodes	15 to 70
Carrier sense range	600m
Malicious node rate	15%
Simulation time	6000s
Packet size	64B
Sybil Ids per malicious node	10
RSS_TIMEOUT	100s
TIME_THRESHOLD	30s
UB_RSS_THRESHOLD	$6.45*10^{-10}$ W
LIST_SIZE	10
CH chosen probability	0.3
Voting time period	10s
Cluster update interval	20s

Table 1: Simulation Parameters

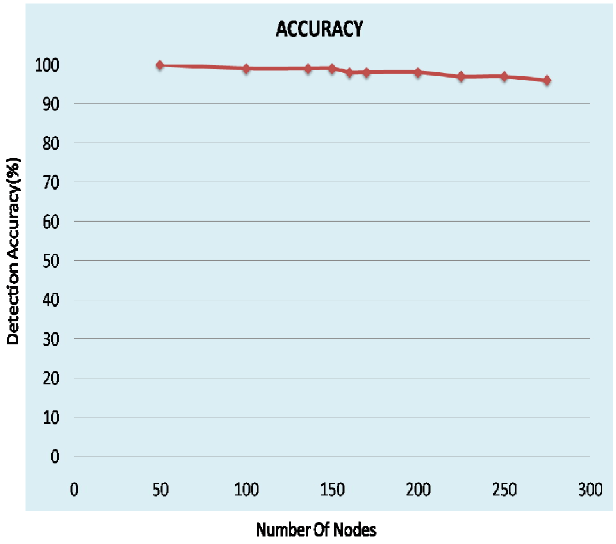

Fig 3: Accuracy rate when True Positive

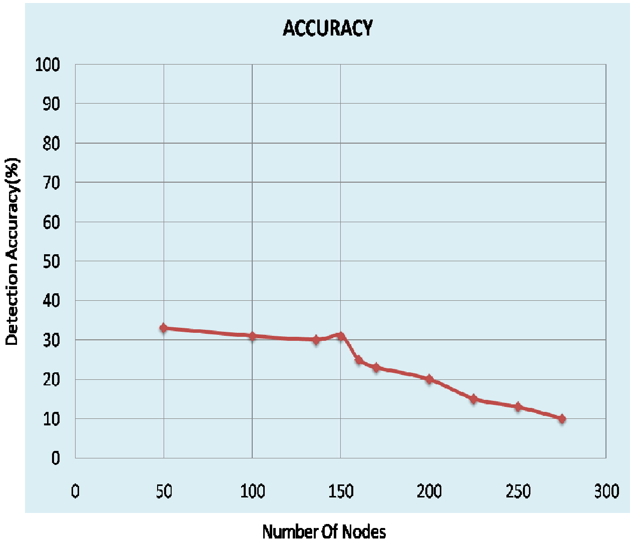

Fig 4: Accuracy rate when False Positive

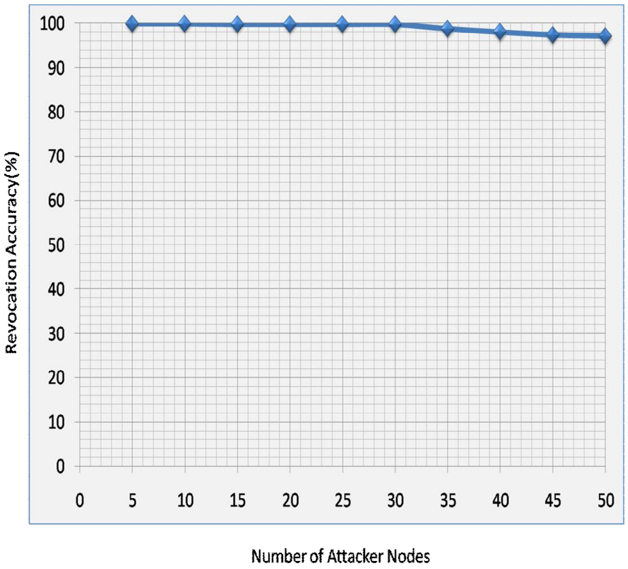

Fig 5: Revocation Accuracy

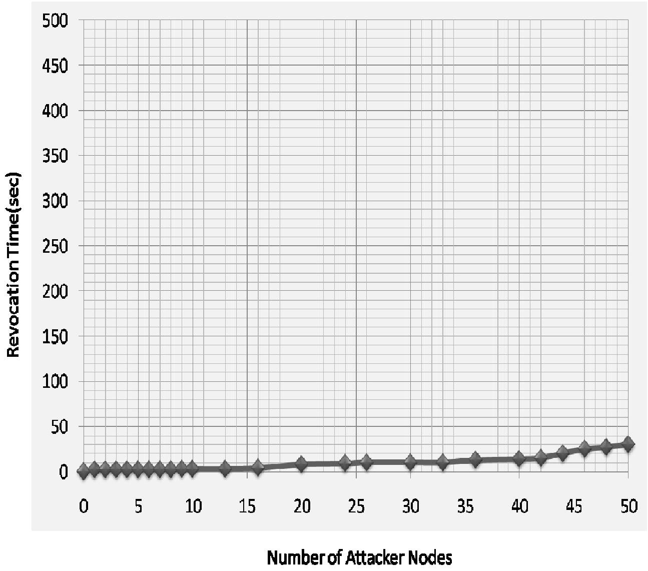

Fig 6: Time elapse when revocation starts

VI. CONCLUSION

The Secure communications within MANETs remain a key issue because of due to high mobility nodes in MANETs. In this paper, to secure the mobile ad hoc networks, we proposed a smart approach RSS and IP based Sybil attack detection method which can produces close to 100% accuracy in identifying Sybil nodes and Certificate invalidation method to overcome Sybil attacker to further participation in the network. The proposed scheme can remove an attacker node by a single node which is nearer to Certification authority and reduces time in notifying as well as in certificate.

ACKNOWLEDGEMENT

I would like to extend my deepest thanks to my guide Mrs. Madhuri T, Assistant Professor, ISE, TOCE, Bangalore who guided me well to put my ideas in this paper.

REFERENCES

[1] J. Douceur, “The Sybil attack," *First International Workshop on Peer-to-Peer Systems*, pp. 251-260, Mar. 2002.
[2] C. Piro, C. Shields, B. N. Levine, (2006), “Detecting the Sybil Attack in Mobile Ad-hoc Networks”, *Securecomm and Workshops*, pp 1-11.
[3] Gilles Guette Sybil Nodes Detection Based on Received Signal Strength Variations within VANET *International Journal of Network Security, Vol.9, No.1, PP.22 {33, July 2009*
[4] M. Demirbas and Y. W. Song, (2006), “An RSSI-Based Scheme for Sybil Attack Detection in Wireless Sensor Networks”, *International Workshop on Wireless Mobile Multimedia (WOWMOM’06)*, New York, USA. pp. 564–570.
[5] K. -F. Ssu, W-T. Wang and W-C. Chang, (2009), “Detecting Sybil attacks in Wireless Sensor Networks using Neighboring Information”, *Computer Networks*, vol. 53, (18), pp.3042-3056.

[6] T. Suen, and A. Yasinsac, “Ad hoc network security: Peer identication and authentication using signal properties," *Systems, Man and Cybernetics (SMC) Information Assurance Workshop*, pp. 432-433, June 2005.

[7] A. Tangpong, G. Kesidis, H. Hung-Yuan, and A. Hurson, “Robust Sybil detection for MANETs,” in *Proc. 18th ICCCN* 2009, pp. 1–6.

[8] K. Park, H. Nishiyama, N. Ansari, and N. Kato, “Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks,” Proc. IEEE 71st Vehicular Technology Conf. (VTC ’10), May 16-19, 2010.

[9] W. Liu, H. Nishiyama, N. Ansari, and N. Kato, “A Study on Certificate Revocation in Mobile Ad Hoc Network,” Proc. IEEE Int’l Conf. Comm. (ICC), June 2011.

[10] J. Lian, K. Naik, and G.B. Agnew, “A Framework for Evaluating the Performance of Cluster Algorithms for Hierarchical Networks,” IEEE/ACM Trans. Networking, vol. 15, no. 6, pp. 1478-1489, Dec. 2007.

[11] J. Kong, X. Hong, Y. Yi, J.-S. Park, J. Liu, and M. Gerla, “A Secure Ad-Hoc Routing Approach Using Localized Self-Healing Communities,” Proc. Sixth ACM Int’l Symp. Mobile Ad hoc Networking and Computing, pp. 254-265. 2005.

BIOGRAPHY

Mr. Suresh N received his Bachelor of Engineering in Information Science and Engineering in 2012. Currently He is a MTech student in Computer Network Engineering from Visvesvaraya Technological University at The Oxford Collage of Engineering, Bangalore. His research interests are Computer Networks and Network Security.

Mrs. Madhuri T received her Bachelor of technology in Computer Science and engineering from Jawaharlal Nehru Technological University. She received her MTech in Computer Science and Engineering from Nagarjuna University .She has 3 years of Industrial experience. Currently she also holds a faculty position as Assistant Professor, Department of ISE, The Oxford College of Engineering.