International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 11 No. 2 Nov. 2014, pp. 520-526

http://www.ijisr.issr-journals.org/

Detection of Sybil Attack using Received Signal Strength and Masquerade Attack using Mutual Guarding

A. Amalorpava Preethi[1] and R. Boopathiraj[2]

[1]Research Scholar,
Department of computer science,
Dr. G R Damodaran College of Science,
Coimbatore-641014, India

[2]Assistant Professor of computer science,
Dr. G R Damodaran College of Science,
Coimbatore-641014, India

ABSTRACT: Mobile Adhoc Networks is one of the complex systems and it is used in many applications and management operations. Due to the difficulties in MANET, it is essential to check the respective node and their security for each, because each node is affected by various attacks and it produces the threats in the network. These threats create more than one identity and it takes the other node's information. The main objective of the proposed work is to detect and eliminate the serious attacks such as Sybil and Masquerade simultaneously.

KEYWORDS: MANET, Sybil, Masquerade, SSC.

1 INTRODUCTION

Nowadays Mobile Adhoc Networks is one of the important researches for challenging the protocol fields. It is the most advanced techniques that are able to communicate without any physical infrastructure and it is one of the fastest, cheapest growing networks with powerful devices [1].

Basically vulnerability of the network is the lack of secure boundaries, limited resources, Cooperativeness, dynamic topology and wireless links. Sometime vulnerability is created by the attackers in the network. The hackers misuse MANET by using the node or changing the identity of the existing nodes. This type of attack is called Sybil Attack and it is the impersonation attack [2, 3].

Sybil attack creates some of the misconception number of nodes present in the networks. These are the malicious nodes. To gain the network of many IP addresses, these attacks are prevented using two approaches. Namely Lightweight Sybil attack detection and robust Sybil attack detection [4].

Some of the goals used to detect these attacks are authentication, availability, integrity, confidentiality and non-repudiation [5].

2 RELATED WORKS

In [6], the implementation of the enhanced property for mobility, that the traffic in the networks is monitored and the results shown the number of networks are detected by Sybil attacks. Here the author extends the protocol to monitor the collision at the media access network of a single attacker.

In [7], the proposed work exploited mobility to enhance security in MANETs. In a fully self-organized MANETs 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.

In [8], a mathematical approach is proposed to detect the Sybil attack. Here the author implemented the framework to detect the vulnerability of ad-hoc routing protocol and this approach is used to analyze the threats in the Sybil attackers by extended strand space mode.

In [9] resources testing are used to identify the Sybil attack through various tasks in the each node of the network.

3 SYBIL ATTACK

Sybil attack provides a lot of damage and creates problem to the networks. Sybil the name comes from that multiple identities and it is named after the famous multiple disorder patient whose name is "Sybil" (Shirley Ardell Mason). This attacker also creates and provides the fake information among the nodes in the whole network and sends the duplicate information among the nodes. Two types of Sybil attack detection is lightweight Sybil attack and robust Sybil attack detection. In both the cases that using parameters are different that first one is based on speed, RSS and cheapest. Second one is based on time, location and expensive.

The Sybil attack is one of the serious problems in MANET and some other application oriented network. So it is important to remove, reduce or eliminate from the network. Usually Sybil attacks are reduced, using cryptographic-based authentication [10 and 11]. But this technique is used in wireless ad hoc network, but for MANET this technique is very difficult to eliminate the Sybil attack. So in this paper, Received Signal Strength is used to protect the network from Sybil attack

4 SIGNAL STRENGTH BASED ANALYSIS

In the proposed implementation, Signal strength analysis is used to find out the distinction between a new legitimate node and a new Sybil identity node. Suppose, if one of the node from the new legitimate is enter into other node means then the first RSS at the receiver node is low. In the Sybil attack that the node creates new identity then the signal strength of this node is high.

It is important to study how each node collects and maintains the RSS values of the neighbouring nodes.

Table 1: Neighboring list based on RSS

Node ID	RSS-List
1	R1-T1---R2-T2---R3-T3---RnTn
2	
3	: : :
N	

The above table provides the list of neighbours in the form, such as <Address, RSS-List <time, rss>. Using protocol such as RTS, CTS, DATA and ACK are used to record the RSS values. Signal strength of the transmission capturing and storing is based on the receiving neighbouring nodes. This can be performed in direct communication that it acts as a source or destination to other nodes or not. Each RSS signal strength has the address R_n RSS and send the data with time period T_n, where n is the number of element in the RSS.

Some of the experiments are used to determine the behaviour of the legitimate node and the Sybil attackers.

Suppose, let us take two nodes, node A and node B. If a new node B enters into the A's neighbourhood or their respective radio range, then the node B takes overtime. It is one of the natural behaviours of the nodes. If node A stays in static position

then the node B enters into their radio range, then B's RSS observes continuously by node A. If it is happened continuously means then the node B is out range and communicates with other nodes.

In this paper based on the threshold the Sybil attack is identified. This type of threshold is depending on the maximum network speed. To identify the speed split the node into two zones that are gray and white node. These partitions are also divided based on the speed based detection. Higher speed thresholds produce the wider gray zones. First node of the gray zones indicates that it is the normal entry of the node in the radio range.

Suppose for example take 12m/s for a normal speed. If any new creation is created of formed in white zone it is denoted as Sybil identity. Smaller speed threshold will work better than the larger ones because they will produce high true positives.

For example, the maximum speed of nodes is 2 m/s in a network, then detection accuracy will be improved only when the detection threshold based on this speed produces narrower gray zone.

Step 1: addNewRss (Address, rss, time−recv)
Step 2: BEGIN SUB:
Step 3: IF: Address is not in the Table
Step 4: THEN:
Step 5: IF: rss >= UB−THRESHOLD
Step 6: THEN: add−to−Malicious−list (Address)
Step 7: Bcast−Detection−Update (Address)
Step 8: ELSE: Add−to−Table (Address)
Step 9: END−IF
Step 10: Create−Record (Address)
Step 11: Push−back (rss, time−recv)
Step 12: IF: list−Size > LIST−SIZE
Step 13: THEN: Pop−front ()
Step 14: END SUB:

The above steps from 1 to 14 is used to detect the Sybil attack, by using addNewsRss function it checks the RSS received signal and the signal time and address. If the address is not present, then it indicates the node is not present in the table and it not communicates or interacts with other before nodes.

UB_THRESHOLD is used to check out whether the RSS transmitter in white zone or not. If it is greater than or equal to the threshold, it denotes the new node in a malicious list. Finally the size of the link is checked with the LIST_SIZE. If it is greater than the LIST_SIZE means that the oldest RSS is removed from the list.

Step 1: IF: RSS−TIMEOUT
Step 2: THEN: rssTableCheck( )
Step 3: rssTableCheck( )
Step 4: BEGIN SUB:
Step 5: FOR: for each Address in the Table
Step 6: DO:
Step 7: Pop−element()
Step 8: IF: (Current−Time—getTime ()) >
Step 9:TIME−THRESHOLD
//Indicating that we did not hear from this Address since the TIME−THRESHOLD
Step 10: THEN:
Step 11: IF: getRss() > UB−THRESHOLD
Step 12: THEN: Add−to−Malicious−List
(Address)
//Indicates previous ID of a Whitewasher
Step 13: ELSE: Print "Normal out of Range"
Step 14: END FOR:
Step 15: END SUB:

The above step is used to control the size and global time called RSS_Timeout. If the time expires then the rssTableCheck is used to check the time for every address and it checks the last received time against the TIME_THRESHOLD. If the time is greater than the threshold it denotes that the respective time is past enough since it has not heard from this node. Now to

check the reason for the perished nodes, the strength of the last RSS is checked against the UB−THRESHOLD. If it is greater, then it indicates the previous identity of a whitewasher; otherwise it is concluded as a normal out of range scenario.

5 MASQUERADE ATTACK

Setting in which an adversary is added to the network and it assumes the id of one of the nodes from 1 to N. In this paper to prevent this attack, two techniques of mutual guarding is used that is sending and receiving of node verification.

5.1 MUTUAL GUARDING

In earlier, nodes are stationary and new nodes are added securely to the network. The immediate neighbour receiving of some packets from someone is called as anomaly. For example two nodes are taken which are s and d and both are communicate in the same area and both are sent packets and received it, these are called mutually guarded.

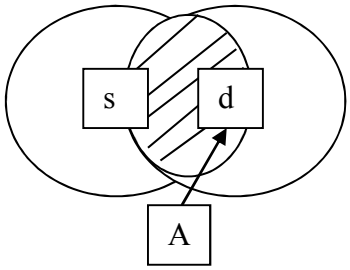

Figure 1: s overhears A masquerading as s

When an adversary A sends a packet to d by setting source id to s, s also receives the packet. S detects the presence of the attacker that masquerades as it. When an adversary is located in the same area then it cannot masquerade as s or d without getting detected. If the node s can transmit, at this time s neighbours are present in the transmission area then the attackers cannot masquerade. Receiving a packet sent by A by changing the source id to s, is an anomaly for a node that has never received a packet from s. id of a node is not neighbour means then it is called as anomaly and can be easily detected.

5.2 VERIFICATION OF THE NUMBER OF PACKETS SENT AND RECEIVED FOR MASQUERADE DETECTION

Using RF, masquerade attack can be detected. The collision is detected if the id of node s transmission data in the time allocated period, then it is an anomaly.

Let us take d be node and s_i denotes the i^{th} neighbor, where i>0 for every T iterations. Then this s_i is used to track the number of sending packets S_{s1d} with the time period for every T iterations. Then d broadcasts a single packet containing the number of packets it received from its neighbours$(R_{s1d}, R_{s2d}, R_{s3d}, \dots)$. If $R_{s1d} > S_{s1d}$, the rule is obtained then the attack of masquerades is present.

6 IMPLEMENTATION WORK

In this paper, implementation of the techniques RSS and mutual guarding is done with the use of Ns2. This tool runs on Linux. It is a simulator tool which has the finest granularity and supports the metropolitan mobility. Ns2 Code contains two sets of languages namely C++ and OTcl (Object Tool Command Language). C++ is used for the creation of objects because of its speed and efficiency whereas OTcl is used as a front end to setup the simulator, configure objects and schedule events. It is easy to use.

The current experiments and simulation results are collected using the Ns2 simulator tool with the backend of C++. AODV (Adhoc On demand Distance Vector routing protocol) defines the coding files such as .h, .cc, and other similar files. The input is given by Tool Command Language and the graph value of animation is extracted using the trace file.

The proposed work shows that the communication between the nodes is secured with the avoidance of Sybil and masquerade attacks.

6.1 EXPERIMENTS AND RESULT

The network consists of 50 nodes.

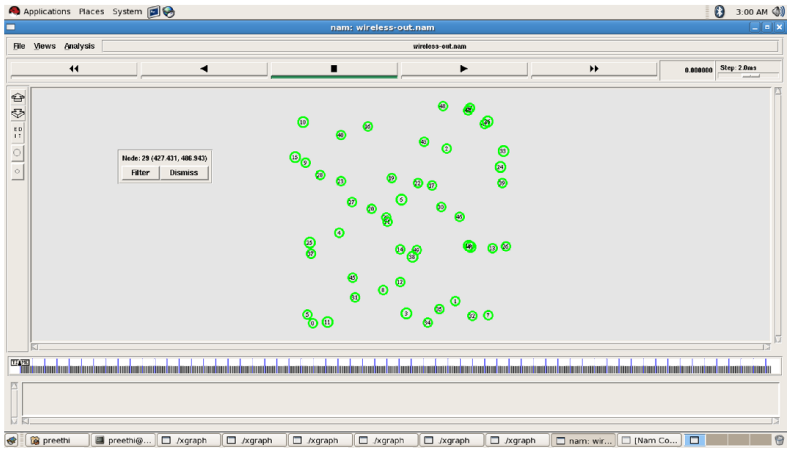

Figure 2: Simulation network

Figure-2 shows the simulation result of nodes communicated from a particular range to another. Out of these fifty nodes, two Sybil nodes and two masquerade nodes has been detected.

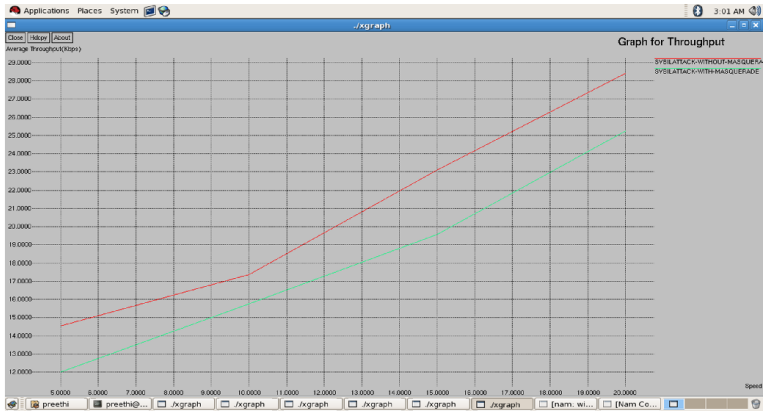

Figure 3: Throughput graph

The number of successful packets delivered through the communication channel is called throughput. The above graph shows the throughput of Sybil without masquerade.

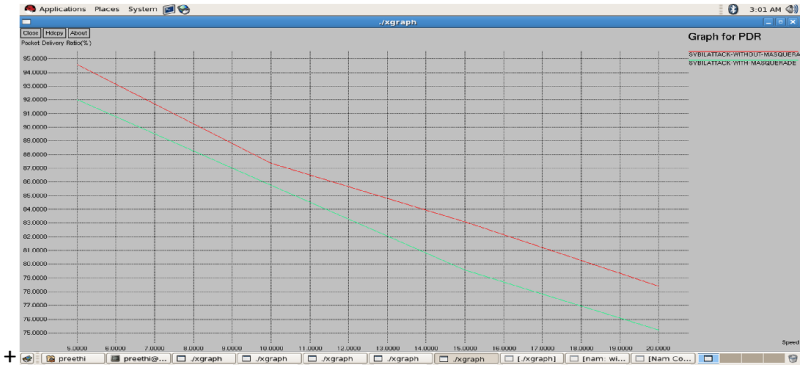

Figure 4: Packet delivery ratio graph

Packet transfer delay is a concept in packet switching technology. The figure-4 shows that the packet delivered is high at the place of Sybil detection without masquerade.

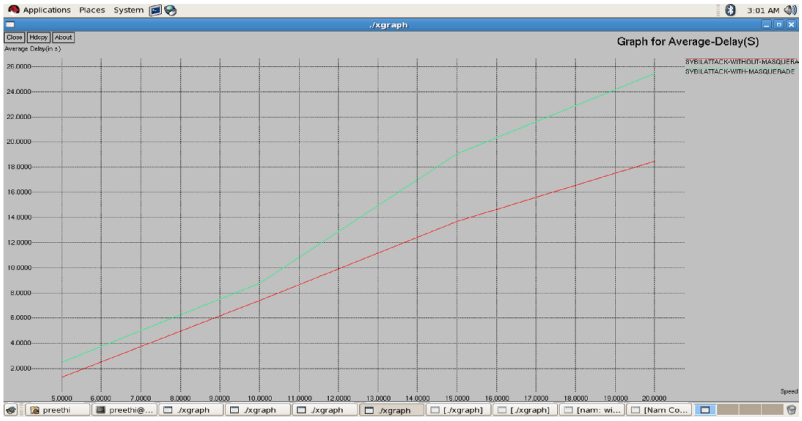

Figure 5: Packet Average delay graph

The above figure shows the delay of packets at the time of sending either due to the link failure or any other defects. Average delay of the packet is high in Sybil without masquerade.

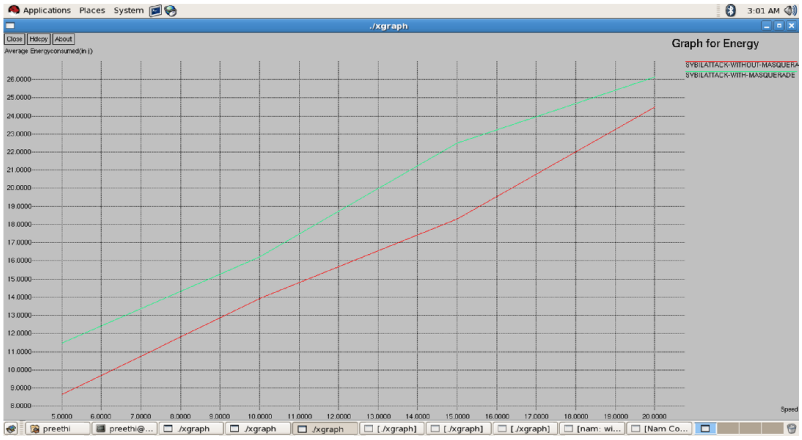

Figure 6: Energy Consumption graph

The energy consumption graph shows that the performance of energy level is low at the detection of both the nodes and it is high in Sybil without masquerade detection.

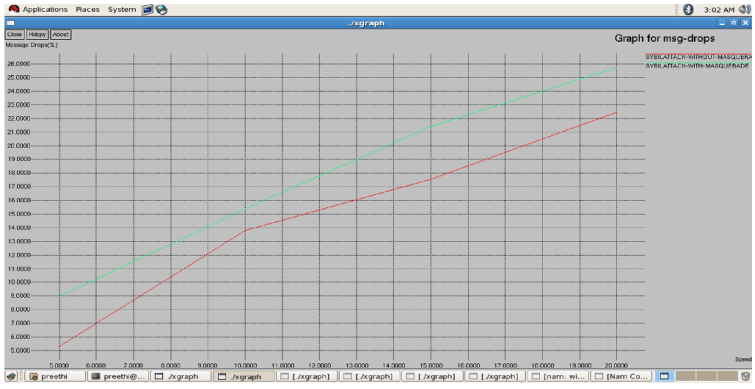

Figure 7: Message drop graph

Figure-7 shows the amount of message drops is detected to be high in Sybil without masquerade.

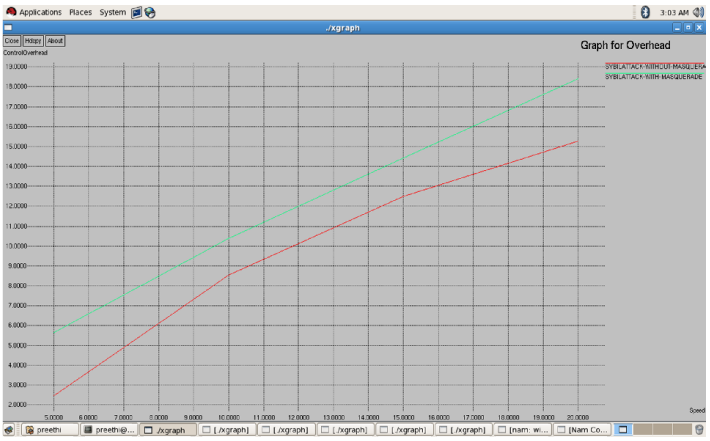

Figure 8: Overhead graph

Figure-8 shows the overhead graph comparison and it shows that the Sybil without masquerade is high.

In figure 3, 4,5,6,7,8 shows that Throughput, Packet delivery ratio, Packet Average delay, Energy Consumption, Message drop and overhead in graph representation. It clearly shows that proposed work is better than previous work.

7 CONCLUSIONS

In this paper, RSS-based detection mechanism and Mutual Guarding techniques are proposed to effectively maintain the network against Sybil attacks and masquerading attack in MANET. The performance level is high while detecting Sybil attacks whereas it is low when both the Sybil and masquerade nodes are detected. Through various experiments that a detection threshold exists for the distinction of legitimate new nodes and new malicious identities is shown. The simulation results showed that the proposed work is better than the existing work even in mobile environments. These detects eliminate the total intrusions over the communication channel of the data link layer.

REFERENCES

[1] Priyanka Goyal, Vinti Parmar and ,Rahul Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Application”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[2] Nirmal Patel and Pratik Modi, “ Detecting Sybil attack using AODV in MANET”, International Journal of Advance Engineering and Research Development (IJAERD) Volume 1,Issue 5,May 2014.

[3] Diogo Miguel da Costa, “Thwarting the Sybil Attack in Wireless Ad Hoc Networks”, Instituto Superior Tecnico.

[4] RoopaliGarg and Himika Sharma, “Comparison between Sybil Attack Detection Techniques: Lightweight and Robust”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 2, February 2014.

[5] LoayAbusalah, Ashfaq Khokar, and Mohsen Guizani, ``A Survey of Secure Mobile Ad Hoc Routing Protocols,'' IEEE Communication Surveys & Tutorials, Vol.10, No.4, pp.78-93, 2008.

[6] Piro, C, Shields, C and Levine, B.N, "Detecting the Sybil Attack in Mobile Ad hoc Networks," Securecomm and Workshops, 2006 , vol., no., pp.1,11, Aug. 28 2006.

[7] S. Capkun, J. P. Hubaux, and L. Buttyan, “Mobility helps peer-to-peer security,” IEEE Trans. Mobile Comput., vol. 5, no. 1, pp. 43–51, Jan.2006.

[8] Gui Jing-jing; Tao Zhang; Zhang Yu-sen, "Modeling and Analyzing the Sybil Attack to Ad-Hoc Routing Protocols," Multimedia Technology (ICMT), 2010 International Conference on , vol., no., pp.1,5, 29-31 Oct. 2010.

[9] D. Monica, J. Leitao, L. Rodrigues, and C. Ribeiro, “On the use of radio resource tests in wireless ad hoc networks,” in Proc. 3rd WRAITS, 2009,pp 21-26.

[10] K. Hoeper and G. Gong, “Bootstrapping security in mobile ad hoc networks using identity-based schemes,” in Security in Distributed and Networking Systems (Computer and Network Security). Singapore: World Scientific, 2007.

[11] S. Hashmi and J. Brooke, “Toward Sybil resistant authentication in mobile ad hoc networks,” in Proc. 4th Int. Conf. Emerging Security Inform., Syst. Technol., 2010, pp. 17–24.