SRAI: Secure Routing For Attacker Identification In MANET

Kothagattu Ramu
Assoc. Prof.
Department of CSE
Siddhartha Institute of Technology and Sciences
Narapally, Hyderabad, Telangana, India

Nampally Prashanth
Asst. Professor
Department of CSE
Siddhartha Institute of Technology and Sciences
Narapally, Hyderabad, Telangana, India

***Abstract*- In the recent years, because of its mobility and scalability, communication has migrated from wired networks to wireless networks. MANET (Mobile Ad hoc Network) is a unique and major application that does not require any pre-existing network infrastructure. When both transmitters and receivers are in the same communication/transmission range, each node can operate as both transmitters and receivers. Otherwise, these nodes rely on neighbor nodes to broadcast their packets, and they have the ability to self-configure, making MANETs popular in critical mission applications like military and other emergency applications. MANETs, in general, are open medium networks with widely spread nodes, making them more vulnerable to numerous attackers. In this instance, it's critical to develop an effective secure routing protocol to protect MANET from a variety of threats. In this study, we will propose and implement the Secure Routing for Attacker Identification (SRAI) routing protocol, which is specifically built for mobile networks. SRAI protocol establishes higher attacker identification rates in particular considerations as compared to existing techniques.**

Key Terms: MANETs, SECURITY, ATTACKS, SRAI protocol.

I.INTRODUCTION

Wireless networks offer flexible mobility and scalability for a variety of communications. As a result, they are always picked for a variety of applications from the start of their development. These wireless networks are regarded as a more advanced technology that has lower communication costs than wired networks, and they have grown in popularity in the fields of research, industry, and academia. MANET (Mobile As hoc Network) is a key wireless network concept that consists of thousands of mobile and self-contained nodes that do not require any existing network infrastructure. The autonomous nodes can freely and randomly migrate within the network, resulting in a transitory dynamic network with regularly changing topology. [1]. The autonomous nodes conduct each activity individually or in tandem, such as node finding and data transfer. MANET nodes are equipped with both a wireless transmitter and a wireless receiver, allowing them to connect with one another over wireless links in a direct or indirect manner, and industrial applications such as remote access and control via wireless links are gaining popularity. The MANET structure is determined by the applications, which can range from small, static networks that demand a lot of power to large-scale dynamic mobile networks. Open and closed mobile networks are the two types of MANETs. Closed mobile networks are typically used for emergency applications such as military and rescue services, and its nodes gather towards a single goal. Different mobile nodes in an open mobile network work toward different goals, but they share common resources to ensure global connectivity. [2,3]. Furthermore, mobile network nodes are capable of providing data communication among multiple users with constant mobility, and after data communication, their mobility is maintained at the same level. The fundamental benefit of a wireless network over a wired network is this. The communication is limited to nodes in varied communication ranges, and mobile nodes can overcome this constraint by allowing intermediary nodes to handle data transmission. This is accomplished by categorizing MANETs into two types of networks: single-hop and multi-hop. A single-hop network is one in which the nodes are in the same communication range and may communicate directly with each other, but in multi-hop networks, the nodes are in different communication ranges and intermediate nodes are chosen for indirect communication. [4,5]. In this instance, the Secure Routing for Attacker Identification (SRAI) protocol, which is specifically built for mobile ad hoc networks, should be proposed.

II. RELATED WORK

Several studies have been carried out in MANETs to identify and resolve security-related concerns, and some of them are provided here that will be relevant in the construction of this study. Abhay Kumar Raiet.al. [6] presented a literature review on MANET attacks, and his work includes a detailed explanation of numerous attacks, as well as

their behaviors and effects on mobile network properties. He also showed how attacks on MANETs are prevented via a technique connected to MANET security. Bing Wu, Jianmin Chen, Jie Wu, and Mihaela Cardei [7] offered further literature of attacks in mobile networks on the same topic. They also talked about security and attack mechanisms. However, the simulation results and mathematical formulae are not provided. Dr.Karim KONATE and GAYE Abdourahime [8] provided several simulation models of many mobile network assaults using NS-2 and discussed routing protocols and their resistances to various attacks portrayed using analytical simulations and mathematical expressions. In the paper [9], proposes an intrusion detection system based on SVM (Support Vector Machine), which is then upgraded to provide superior security. In order to reduce the packet size (training data size), data is preprocessed and comparable data is excluded using k means clustering, as proposed in [10], which shows a significant reduction in training time while maintaining accuracy. The selection of parameters is an important aspect of classification because some features may be excessive or require little effort in the detection process. Farah Jemili et al. [11] introduced a Bayesian Network (BN) based intrusion detection scheme, which is used to build an automatic intrusion detection system based on signature recognition. The goal is to discern signatures of known attacks and match them with the signatures that have been found. Signal infiltration happens if it is similar. Gholam Reza Zargar and Peyman Kabiri [12] wanted to know how to extract efficient network parameters in order to detect network intrusion.

III. PROPOSED PROTOCOL

We proposed the Secure Routing for Attacker Identification (SRAI) protocol in our paper, which mechanically generates a misbehavior report to communicate the status of the obtained packets to the corresponding source, and this SRAI protocol conceives the threshold value of the transferred node that can be used to discover the original packets at the destination side. Take, for example, a node with a threshold value of 30 that ensures the threshold value when it reaches the receiver side. If the checked threshold value remains constant, the destination assumes ownership of the delivered packet and sends an acknowledgement to the source. If any assailants watch or alter these sent packets on their route to their target, the threshold value may change, and it is then forwarded to the destination, which confirms the threshold value and detects the received packet is replicate. The destination then sends a misbehavior report to the source node in question.

DESCRIPTION

A mobile network often consists of thousands of mobile nodes, each of which operates as a source capable of sending packets across the network, a receiver capable of receiving packets, and a router or agent capable of forwarding messages. When packet transmission occurs, the router or agent node transmits the packets from source to destination, and the destination generates an acknowledgement for the corresponding node, which is forwarded to the sender to inform them of the status (such as dropped or received) of the transmitted packets. Only after the source obtains an acknowledgement for received packets may it send a further packet to the destination through the network. If a sent packet is corrupted, hacked, or modified by an attacker on its way to its destination, the attacker's modified packet is likewise sent to the recipient.

We propose a protocol called Secure Routing for Attacker Identification (SRAI) that automatically generates a misbehavior report to relay the status of the received packets to the source in order to identify the attacked or modified packets at the receiver side. This SRAI protocol takes into account the transmitted node's threshold value, which can be utilized to detect the proper packets at the receiver end. Consider the case of a node with a threshold value of 50. It checks the threshold value when it arrives at its destination. If it is constant, the receiver assumes the packet it has received is original and sends an acknowledgement to the sender. If an attacker views or modifies packets on their way to their destination, the threshold value may change, and the packets are then forwarded to the destination, which checks the threshold value and determines the received packet is duplicate. It then sends a report to the source about the misbehavior.

IV. EXISTING METHOD ISSUES

- It lacks security during packet transmission, and we can't easily identify attacked packets or attackers utilizing such methods.
- The network's destination can accept packets containing a certain number of attacked packets.
- Using traditional methods, no acknowledgement of the status of received packets is generated.
- The overall network's throughput and efficiency are degraded.

V. ADVANTAGE OF PROPOSED METHOD

- We can readily identify the attacked packets and attackers using our proposed protocol, which provides additional security while in transmission.
- When the SRAI protocol gets attacked packets, it can create a misbehavior report.
- When compared to previous approaches, the throughput and efficiency of the entire network is enhanced.

VI. EXPERIMENTAL RESULTS

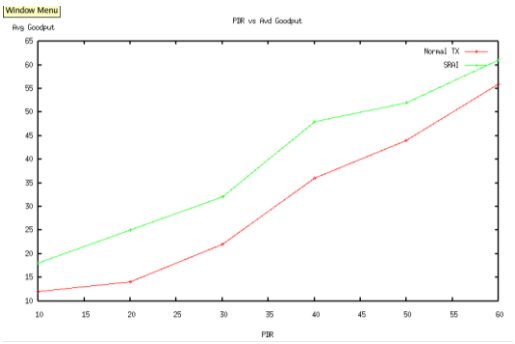

Fig 1: Comparison between PDR and Good put of Normal transmission and SRAI protocol

Figure 1 shows the performance of networks that employ the SRAI protocol vs networks that use standard transmission, with a focus on packet delivery ratio and excellent put. The SRAI protocol is used in a network with a high PDR and good put.

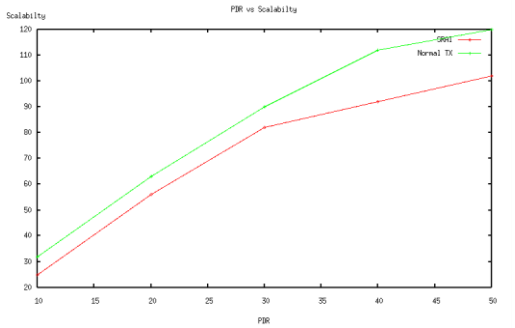

Fig 2: Comparison between PDR and Scalability of Normal transmission and SRAI protocol

Figure 2 shows the performance of networks that employ the SRAI protocol vs networks that use standard transmission, with a focus on packet delivery ratio and scalability. The SRAI protocol is used in a network with a high PDR and scalability.

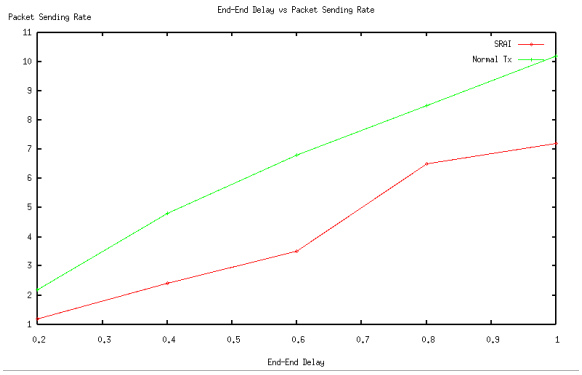

Fig 3: Comparison between End-to-End delay and packet sending rate of Normal transmission and SRAI protocol

We compare the performance of networks that utilize the SRAI protocol and networks that use standard transmission in Figure 3, focusing on end-to-end delay and packet sending rate. The SRAI protocol is used in a network that has a low end-to-end delay and packet sending rate.

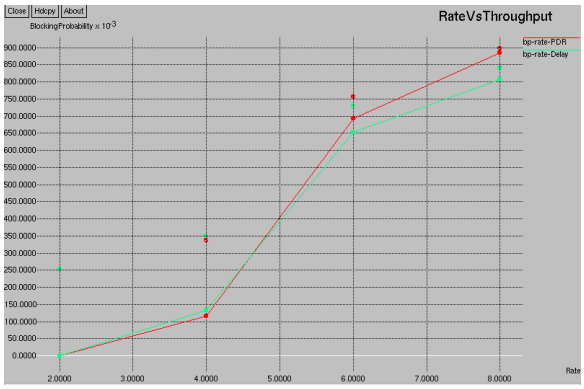

Fig 4: Comparison between Rate and Throughput of Normal transmission and SRAI protocol

Figure 4 shows the performance of networks that use the SRAI protocol vs networks that use standard transmission, with a focus on packet delivery rate and throughput. PDR and throughput are both high in the SRAI network.

VII. CONCLUSION

Packet dropping or hacking are serious security threats in MANETs, so we suggested the Secure Routing for Attacker Identification (SRAI) protocol, which is built specifically for mobile ad hoc networks. We can detect attacked nodes at the receiver side using the SRAI protocol by considering its threshold value, and it automatically generates a misbehavior report to the source. When compared to various existing attacker or intruder identification systems, we found that our proposed SRAI protocol outperforms them. We will continue to work on improving the security of MANETs by integrating some authentication protocols in the future.

VIII. REFERENCES

[1] H. Miranda and L. Rodrigues, ―Preventing Selfishness in Open Mobile Ad Hoc Networks,‖ Proc. Seventh CaberNet Radicals Workshop, Oct. 2002.

[2] Y. Kim, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," IEEE Trans. Instrum.Meas., vol. 57, no. 7, pp. 1379–1387, Jul. 2008.

[3] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.

[4] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[5] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[6] Abhay Kumar Rai, Rajiv RanjanTewari and Saurabh Kant Upadhyay "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3).

[7] Bing Wu, Jianmin Chen, Jie Wu andMihaelaCardei "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", wireless/mobile network security, 2006 Springer.

[8] DrKarim KONATE and GAYE Abdourahime "Attacks Analysis in mobile ad hoc networks: Modeling and Simulation", 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, 2011 IEEE.

[9] Jingbo Yuan , Haixiao Li, Shunli Ding and Limin Cao "Intrusion Detection Model based on Improved Support Vector Machine", Third International Symposium on Intelligent Information Technology and Security Informatics, 2010 IEEE.

[10] Z. Muda, W. Yassin, M.N. Sulaimanand N.I.Udzir"Intrusion Detection based on K-Means Clustering and OneR Classification", 2011 IEEE.

[11] Farah Jemili, Dr. MontaceurZaghdoud and Pr. Mohamed Ben Ahmed "A Framework for an Adaptive Intrusion Detection System using Bayesian Network", 2007 IEEE.

[12]http://link.springer.com/chapter/10.1007%2F978-3-642-14400 4_50?LI=true#.