IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Manet Security and Attacks Issues, Challenges & Solutions

K. Sumathi[1*], D. Vimal Kumar[2]

[1,2]Department of Computer Science, Nehru Arts and Science College, Coimbatore, India

[*]*Corresponding Author: sumathiisri5@gmail.com, Tel.: 8220470591*

DOI: https://doi.org/10.26438/ijcse/v7i3.433437 | Available online at: www.ijcseonline.org

Accepted: 05/Mar/2019, Published: 31/Mar/2019

***Abstract*—** The mobile ad hoc network, security has been active research topic but due to self-configuring characteristics of mobile ad hoc network there are numerous like shared wireless medium with open network design, limited resources, dynamic network topology and many more that hinder to maintain the security of the wireless network. Because of MANET's properties like infrastructure-less and self-configuring, there are more risks for trusted nodes to be compromised and start attack on networks. It is hard to recognize between stale routing and faked routing data on account of node mobility system. In node mobility mechanism it authorizes frequent networking reconfiguration which makes more risks for attacks. Due to limited power consumption and computation capability mobile devices are helpless against the blackhole and grey hole attack as they are inadequate to run security algorithms which require high computations like public key algorithms. In this problem consider as a propose system the power and delay optimization protocol may be integrated to improve the performance of the network. The delay aware hash-based message authentication code (D-HMAC) used to secure the packet sending between source to destination without greyhole and blackhole attacks. The experimental result using NS2 simulation the proposed algorithm achieves better performance and attack detection accuracy than the existing trust level methods.

***Keywords*—** Mobile Ad-hoc Network, Security Issues, Routing Protocols, Attacks.

I. INTRODUCTION

In a MANET, nodes within one another's wireless transmission range can communicate directly; however, nodes outside one another's range have to rely on some other nodes to relay messages. Thus, a multi-hop scenario occurs, where several intermediate hosts relay the packets sent by the source host to make them reach the destination node. MANET is one that comes together as needed, not necessarily with any support from the existing infrastructure or any other kind of fixed stations. This statement can be formalized by defining an ad hoc network as an autonomous system of mobile hosts (MHs) (also serving as routers) connected by wireless links, the union of which forms a communication network modeled in the form of an arbitrary communication graph. This is in contrast to the well-known single hop cellular network model that supports the needs of wireless communication by installing base stations (BSs) as access points. In these cellular networks, communications between two mobile nodes completely rely on the wired backbone and the fixed (BSs). In a MANET, no such infrastructure exists and the network topology may dynamically change in an unpredictable manner since nodes are free to move.

MANET's unique characteristics make it affected by several types of attacks. Since they are used in an open environment where all nodes can change their position at any time to some other place, all the nodes should co-operate to forward the packets in the network. So, detecting the malicious nodes is also a difficult task in MANET. Hence, it is relatively difficult to design a secure protocol for MANET, when compared to wired or infrastructure–based wireless networks.

II. ATTACKS ON EXISTING PROTOCOLS

The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Examples of passive attacks are snooping, eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonation, modification, denial of service (DoS), and message replay.

The attacks can also be classified into two categories, namely external attacks and internal attacks, according to the domain of the attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks

are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

Physical layer attack: Eavesdropping is the intercepting and reading of messages and conversations by unintended receivers. The mobile hosts in mobile ad hoc networks share a wireless medium. The majority of wireless communications use the RF spectrum and broadcast by nature. Signals broadcast over airwaves can be easily intercepted with receivers tuned to the proper frequency. Thus, messages transmitted can be eavesdropped, and fake messages can be injected into network. Moreover, a radio signal can be jammed or interfered, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. The most common types of this form of signal jamming are random noise and pulse. Jamming equipment is readily available. In addition, jamming attacks can be mounted from a location remote to the target networks.

Link Layer Attack: The MANET is an open multipoint peer-to-peer network architecture. Specifically, one-hop connectivity among neighbors is maintained by the link layer protocols, and the network layer protocols extend the connectivity to other nodes in the network. Attacks may target the link layer by disrupting the cooperation of the layer's protocols.

Network Layer Attack: Network layer protocols extend connectivity from neighboring 1-hops nodes to all other nodes in MANET. The connectivity between mobile hosts over a potentially multi-hop wireless link strongly relies on cooperative reactions among all network nodes. A variety of attacks targeting the network layer have been identified and heavily studied in research papers. By attacking the routing protocols, attackers can absorb network traffic, inject themselves into the path between the source and destination, and thus control the network traffic flow.

Wormhole attack: An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages is tunneled. This tunnel between two colluding attackers is referred to as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

Black hole attack: The black hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks. There is a subtler form of these attacks when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrongdoing.

Byzantine attack: A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

Rushing attack: Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne.

III. SECURITY ISSUES IN NAMET

MANETS do not have any centralized control facility which may lead to many security problems. It becomes very difficult to detect any attack. Traffic cannot be monitored from a centralized point; instead the control is distributed at each node. The detection becomes more difficult when the advisory changes the attack pattern and the target of the attack. To the node a failure may be caused by an adversary or due to some network problem. Due to the lack of security association, we cannot classify the nodes as trusted node or untrusted node.

To provide better detection performance, it is necessary to analyses and categories MANET attack models and system vulnerabilities. Sufficient research into the attack scenarios is necessary in several respects as existing research work lacks any such If a new kind of attack takes place whose behavior is unknown it will be difficult to identify the node and isolate from the system.

- To integrate a model at the appropriate layer with a suitable process model need to integrate a detection engine that identifies an attacker in a generalized way instead of identifying them according to their category.

- The power optimization protocol may be integrated to improve the performance of the network.
- The cross-layer integration can also be included for other layers to further optimize the performance of the networks further.
- Computational and Power Limitations prevent the use of complex Encryption Algorithms.

IV. PROPOSE SOLUTION

Mobile ad hoc networks (MANETS) is defined as wireless networks that have continuously self-organized nodes though these nodes are connected with each other in wireless manner. There no any centrality maintains and controlling. The MANET routing protocol is difficult to maintain the link because it self-organizing and self-configuring multi-path wireless network it dynamically changes node location frequently. The MANETs are use many applications outdoor events, communications in regions with no wireless infrastructure, emergencies and natural disasters, and military operations, mine site operations, urgent business meetings and robot data acquisition. In MANET one of the major problems is data security. In existing many algorithms to solve this problem.

The infrastructure less network, battery constraint and the non-cooperative environment it is difficult to provide security to the network. Some nodes try to save their energy and start to exhibit malicious activities like dropping the packet by not forwarding etc. Due to such security problems in the network, the routing also becomes inefficient. The different security mechanisms are compared in order to check their effectiveness in handling network attack problems. Most previous and recent ad hoc networks have already focused on providing routing services without considering any high-level security and delay aware routing based on optimization technique. The secure communication and minimum delay in mobile ad hoc network, research direction will be focused on capabilities on path delay estimation and co-operation of neighboring nodes.

The propose approach is based on delay aware hash-based message authentication code (D-HMAC). The proposed security mechanism prevents malicious nodes from tampering or replaying intermediate packets by means of signing and encrypting the packet at each intermediate trusted node. The proposed routing technique achieves in terms of End-to-End Delay, Throughput, and Network Lifetime. By NS2 simulation results the proposed algorithm achieves better performance than the existing methods.

V. COMPARISION OF EXISTING SYSTEMS

Different mechanisms have been proposed in the literature using various cryptographic techniques to countermeasure the routing attacks against MANET. However, these mechanisms are not suitable for MANET resource constraints, such as dynamic topology, limited bandwidth and constraints on power utility. Hence, they introduce heavy traffic load to exchange and verify keys. The research work investigates the current security issues in MANET in specific to study and analyze the various routing layer attacks and MAC layer attacks, such as flooding, black hole, wormhole, packet replication and route cache poisoning attacks, as well as defense mechanism to protect from those attacks.

The overall goal of the security solutions for MANET is to provide security services including authentication, confidentiality, integrity, nonrepudiation and availability to the mobile users. In order to achieve these goals, the security solution should provide complete protection spanning the entire protocol stack. So, malicious attack must be deployed to detect attacks against the routing infrastructure. At the same time, the requirement for detection of attacks against a mobile node in a wireless ad-hoc network is the same as for hosts in a fixed wired network. But a MANET node typically has limited battery power; it is not efficient to always make each MANET node the monitoring node for itself to detect all these attacks. Then, the monitors can only be placed at some key points instead of at every node. Therefore, in order to gain high performance and make effective detection, it is important to investigate distributed monitoring mechanism appropriate for ad hoc networks.

VI. RECENT SECURITY SOLUTION FOR MANET

Table 1. Comparison of existing methods and remarks

S. No	Paper Title	Problems	Solutions
1	Energy-Aware Path Construction for Data Collection Using Mobile Sink in Wireless Sensor Networks	Energy imbalance problem.	Data collection can be improved
2	Secure Distributed Estimation over Wireless Sensor Networks under Attacks	Presence of attacks on sensed and communicated information	Received information from the trust neighbors. The mean and mean-square senses are analyzed, and then an adaptive rule is suggested to select the threshold for detection.
3	Stable Energy efficient QoS based Congestion and Delay aware Routing (SEQCDR) Protocol for MANETs	Mobility and congestion of the nodes lead to frequent link failures and packet losses.	Energy efficient QoS based Congestion and Delay aware Routing (SEQCDR) Protocol for effective QoS support.
4	Importance of on-demand modified power aware dynamic source routing protocol in mobile ad-hoc networks	Does not take the battery power limitation of the MANET nodes into account.	Efficient power routing DSR (EPRDSR) to improve the power efficient scheme in the whole MANET
5	Energy Efficient Multipath Routing Protocol for Mobile ad-hoc Network Using the Fitness Function	Energy consumption is considered as one of the major limitations in MANET, as the mobile nodes do not possess permanent power supply and have to rely on batteries, thus reducing network lifetime as batteries get exhausted very quickly as nodes move and change their positions rapidly across MANET.	The fitness function is used to find the optimal path from the source to the destination to reduce the energy consumption in multipath routing.

VII. CONCLUSION

In node mobility mechanism it authorizes frequent networking reconfiguration which makes more risks for attacks. Due to limited power consumption and computation capability mobile devices are helpless against the blackhole and grey hole attack as they are inadequate to run security algorithms which require high computations like public key algorithms. In this problem consider as a propose system the power and delay optimization protocol may be integrated to improve the performance of the network. The delay aware hash-based message authentication code (D-HMAC) used to secure the packet sending between source to destination without grey hole and blackhole attacks.

REFERENCES

[1] Weimin Wen,et al., "EAPC: Energy-Aware Path Construction for Data Collection Using Mobile Sink in Wireless Sensor Networks" IEEE SENSORS JOURNAL, VOL. 18, NO. 2, JANUARY 15, 2018

[2] Ying Liu et al., "Secure Distributed Estimation over Wireless Sensor Networks under Attacks" IEEE Transactions on Aerospace and Electronic Systems (Volume: 54 , Issue: 4 , Aug. 2018)

[3] Shoubai Xiao "Security Analysis and Application of Common Dynamic Routing Protocol", 7th International Conference on Education, Management, Computer and Society (EMCS 2017)

[4] Mandeep Kaur Gulati "Stable Energy efficient QoS based Congestion and Delay aware Routing (SEQCDR) Protocol forMANETs" 2015 International Conference on Communications and Signal Processing (ICCSP) 2-4 April 2015

[5] Shiva Shankar "Importance of on-demand modified power aware dynamic source routing protocol in mobile ad-hoc networks" IET Microwaves, Antennas & Propagation (Volume: 8 , Issue: 7 , May 14 2014)

[6] Shivashankar "Implementing a new power aware routing algorithm based on existing dynamic source routing protocol for mobile ad hoc networks", IET Networks (Volume: 3 , Issue: 2 , June 2014)

[7] Mueen Uddin "Energy Efficient Multipath Routing Protocol for Mobile ad-hoc Network Using the Fitness Function" IEEE Access (Volume: 5) 24 May 2017.

[8] A.Siddiqua, S.Kotari, and AAKhan Mohammed. "*Preventing black hole attacks in MANETs using secure knowledge algorithm*", Signal Processing and Communication Engineering Systems (SPACES), 2015 International Conferenceon. IEEE, **2015**.

[9] N.Choudhary and L.Tharani. "*Preventing black Hole attack in AODV using timer-based detection mechanism*", Signal processing and communication engineering systems (SPACES), 015 international conferenceon. IEEE**,2015**.

[10] AK Jain and V Tokekar. "*Mitigating the effects of Black hole attacks on AODV routing protocol in Mobile adhoc Networks*", Pervasive computing (ICPC), 2015 international conference on. IEEE, **2015**.

Authors Profile

I K. Sumathi had received M.Sc Computer Science at STC College, Bharathiar University from the Department of Computer Science, India, in 2013 wih gold medal. I had completed M.Phil Computer Science at Sree Saraswathi Thyagaraja College of arts & Science College, Bharathiar University in the Year 2014. I have 3.5 years of teaching experience. My area of interest are networking, Data Mining and Image Processing . Now I am pursing part time Ph.D in Computer Science under the guidance of

D. Vimal Kumar.

D. Vimal Kumar received MCA degree at KSR College of Technology, Periyar University from the Department of Master of Computer Applications, India, in 2002. He received his M.Phil Computer Science degree at Kongu arts & Science College, Bharathiar University in the Year 2007. He received his doctorate in Anna University in the year 2014. He has 14 years of teaching experience. He is one of the approved supervisor of Bharathiar University currently guiding 06 scholars. He has published 17 articles in National /International journals. He has also presented papers in National and International Conferences. His area of interest includes data mining, network, software engineering, mobile computing and image processing. He is currently working as Associate professor in department of computer science in Nehru Arts and Science College, T.M Palayam, Coimbatore, Tamilnadu, India.

