Volume 4, Issue 11, November 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Attacker Misbehavior and Security Schemes to Protect MANET: A Survey

Gajendra Singh
HOD of Computer Science & Engineering
Sri Satya Sai Institute of Science &Technology
Sehore (M.P.), India

Amrita Gayakwad
Department Of Computer Science & Engineering
Sri Satya Sai Institute of Science &Technology
Sehore (M.P.), India

Abstract -Security has become a critical issue between the mobile nodes in MANET. MANET is generally more prone to physical security attacks and threats than the fixed- cable networks. The inherent characteristics of MANET such as wireless medium, highly dynamic topology, distributed cooperation, resource constrained capability, and limited physical security poses number of nontrivial security challenges to the network. Hence, enforcement of security through secure routing protocol becomes an extremely critical task. Non-optimal routes are results of malicious modification through attacker and inconsistent routing information exchange by attacker during packet forwarding. Due to highly dynamic nature of MANET link breaks and new path have to be searched which may not be optimal. In this paper, an effort has been made to concentrate on the malicious of different attacks and security schemes proposed by various researchers and also proposed the some new approach against wormhole attack in MANET.

Index Terms—Security, MANET, Routing, Attack, Survey

I. INTRODUCTION

Mobile Ad-Hoc Network (MANET) is an infrastructure less collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies and random mobility with constrained resources. They also have capability of network partition. A mobile ad hoc network (MANET) is a self-organized multi-hop system comprised of mobile wireless nodes.

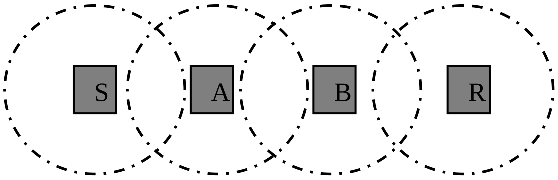

Fig.1 Example of MANET

Two nodes out of direct communication range need intermediate nodes to forward their messages shown in figure 1. The Sender S has communicate with Receiver R through intermediate nodes A and B. Common applications of MANET are: military or police networks, business operations like oil drilling platforms or mining operations and emergency response operation such as after natural disaster like a flood, tornado, hurricane and earthquakes. Due to multi-hop routing and open working environment, MANETs are vulnerable to attacks by selfish or malicious nodes, such as packet dropping (black-hole) attacks and selective forwarding (gray-hole) attacks. Wormhole attack is a type of attack that are work as to established path in between sender and receiver but if the sender has start data transmission then in that case the worm hole attacker has create a direct link, referred to as a wormhole tunnel between them, it means more of the number of trusted nodes it means higher successful data communication process rates may well expected. In this desertion we proposed detection as well as prevention technique against wormhole attack, for detection we use profile base detection technique and get attacker node information like node number, number of attack packet, attack time etc. after that we prevent wormhole attack using neighbor trust worthy base technique and secure the mobile ad-hoc network communication, through our proposal we provide secure as well as reliable communication and simulate through network simulator-2 and analyze the network behavior in attack and prevention case. After that we measure the performance of network on the bases of network parameter like throughput, packet delivery ratio, throughput, routing load etc.

II. ROUTING PROTOCAL DESCRIPTION

There are basically three types of routing protocols:

Proactive protocols In networks utilizing a proactive routing protocol, every node maintain one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain up-to-date routing information from each node to every other node. To maintain up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis which in turn leads to relatively high overhead on the network. The advantage is that routes will always be available on request.

Reactive protocols Unlike proactive routing protocols, reactive routing protocols do not make the nodes initiate a route discovery process until a route is required. This leads to higher latency than with proactive protocols, but lower overhead.

Hybrid protocols each node maintains both the topology information within its zone and the information regarding neighboring zones that means proactive behavior within a zone and reactive behavior among zones. Thus, a route to each destination within a zone is established without delay, while a route discovery and a route maintenance procedure is required for destinations that are in other zones.

III. SECURITY ISSUSE FOR MANETS

Vulnerabilities of operating systems and upper layer applications that belong to user programs such as databases, browsers, or client-server applications are not considered as a security issue for ad hoc networks. General attack types are the threats against the routing layer of the MANET such as physical, MAC and network layer which is the most important function of wireless ad-hoc network for the routing mechanism, orienting the packets after a route discovery process. Other vulnerabilities are application security, network security, database security which are studied in different works which are not explained in detail here. Attacks to the wireless ad-hoc network in the networking layer usually have two purposes: not forwarding packets or adding and changing some parameters of routing messages; such as sequence number and IP addresses. These will be detailed in the subsequent sections. Using one of the key mechanisms such as cryptography or authentication, or both in a network, serves as a preventive approach and can be employed against '*attackers*'. However, these mechanisms protect the network against attacks that come from outside, malicious '*insiders*' which use one of the critical keys can also threaten the security. For instance, in a battle field where MANET are used, even if keys are protected by temper proof hardware that are used in the vehicles in the network, it is difficult to say that these vehicles exhibit the same behavior if the enemy captures them. On the other hand, a node may un-deliberately misbehave as if it is damaged. A node with a failed battery which is unable to perform network operations may be perceived as an attack. Another malicious behavior of the nodes is selfishness. Selfish nodes refrain from consuming its resources; such as battery, by not participating in network operations. Therefore, failed and selfish nodes also affect the network performance as they do not correctly process network packets, such as in routing mechanism. We should, therefore ensure that everything is correctly working in the network to support overall security and know how an insider is able to attack the Mobile ad hoc network. Wireless ad-hoc networks should be protected with an intrusion detection system that can understand the possible actions of attackers and can produce a solution against these attacks.

IV. TYPE OF ATTACKS

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network. The attacks in MANETs are divided into two major types. Network either as internal, external or/ as well as active or passive attack against the network.

The connectivity of mobile nodes over a wireless link in MANETS which is multi hop in nature strongly relies on the fact that ensures cooperation among the nodes in the network. Since network layer protocols forms connectivity from one hop neighbors to all other nodes in MANET, the assurance of cooperation among nodes is required. The attacks in MANETS are classified into two major categories, namely passive attacks and active attacks, according to the attack means [2]. Passive attacks are those, launched by the adversaries solely to snoop the data network. Such attacks identification becomes very difficult since network itself does not affected and they can reduced by using powerful encryption techniques. But an active attack tries to alter or destroy the information that is being exchanged, thereby disturbing the normal functionality of the network exchanged in the network. These adversaries in any way don't disturb the operation.

a) Impersonation

A malicious node can launch many attacks in a network by masquerading as another node (Spoofing). Spoofing occurs when a malicious node misrepresents its identity and the traffic that belongs to the impersonated node is redirected to the malicious node.

b) Modification

A malicious node may attack by altering the protocol fields of messages passed among the nodes. Malicious node can easily cause traffic subversion and denial of service by setting the false values of various fields in the packet such as route sequence numbers.

c) Fabrication

In such type of attack, an attacker or malicious node generates the false routing information. Because the routing constructs comes as valid so such kind of attacks are difficult to indentify. For example, a false RERR route error message can be generated by an attacker, which claims that a neighbor can no longer be contacted.

d) Wormhole Attack

In this type of attack, two colluding malicious nodes create a tunnel between them using a private high speed network(s). This attack allows a node to short-circuit the normal flow of routing message. The attacker at one end collects the data and replays them at the other end using tunnel.

e) Black hole Attack

An intruder can launch this attack by sending false routing information and advertise itself as having an optimum path to the destination node. For example, a malicious node can reply for route request falsely without having an active route to the destination and causes other good nodes to route data packets through the malicious node.

f) Denial of Service (DoS)

The first type of attack is denial of service, which aims to crab the availability of certain node or even the services of the entire ad hoc networks. In the traditional wired network, the DoS attacks are carried out by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable. Nevertheless, it becomes not practical to perform the traditional DoS attacks in the mobile ad hoc networks because of the distributed nature of the services. Moreover, the mobile ad hoc networks are more vulnerable than the wired networks because of the interference-prone radio channel and the limited battery power. In the practice, the attacker packet delivering from predefined path.

V. PREVIOUS WORK HAS BEEN DONE

Pallavi Sharma and Aditya Trivedi proposed an Approach to Defend against Wormhole Attack in Ad Hoc Network Using Digital Signature [1]. They present a mechanism which is helpful in prevention of wormhole attack in ad hoc network is verification of digital signatures of sending nodes by receiving node because each legitimate node in the network contains the digital signature of every other legitimate nodes of same network. A wormhole is one of prominent attack which is formed by two malicious nodes and a tunnel. In order to protect from wormhole attack we used the scheme called multi hop count analysis (MHA) with verification of legitimate nodes in network through its digital signature. Destination node analyzes the number of hop count of every path and selects the best path for replying. In this solution, if sender wants to send the data to destination, firstly it creates a secure path between sender and receiver with the help of verification of digital signature. If there is presence of any malicious node in between the path then it is identified because malicious node does not have its own legal digital signature.

Hussain et al [6] proposed Denial of Service Attack in AODV & Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Adhoc Network. In this work Denial of Service attack is applied in the network, evidences are collected to design intrusion detection engine for MANET Intrusion Detection System (IDS). Feature extraction and rule inductions are applied to find out the accuracy of detection engine by using support vector machine. True Positive generated by the detection engine is very high and False Positive is suppressed to negligible. True positive will be reported very fast in Lids & Friend list generated by Lids will be sent to the Gids module for further investigation. Global Detection Engine will generate the friend list according to trust level, higher the trust level of the node may be used for other different processes like routing, and deciding the cluster head for scalable ad-hoc networks. Feature extracted for Routing parameters and MANET Traffic generation parameters can be used for different routing protocols. For detection engine machine learning algorithm Support Vector Machine is used which is light weighted and considered best among the supervised learning algorithms, prediction (accuracy) generated by the SVM for input features and different values of C & λ to established the system for given training and testing data sets are satisfactory.

Jing-Wei Huang et al [7] proposed Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks. In this work uses a trust based multipath AOMDV routing combined with soft encryption, yielding our so-called T-AOMDV scheme More precisely, this approach consists of three steps: (1) Message encryption – where at the source node, the message is segmented into three parts and these parts are encrypted using one another using some XOR operations, (2) Message routing – where the message parts are routed separately through different trust based multiple paths using a novel node disjoint AOMDV protocol, and (3) Message decryption – where the destination node decrypts the message parts to recover the original message.

Shreenath et al [8] proposed Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs. This work focus on improving the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to safeguard it against flooding and blackhole attacks. The proposed mechanism is for flooding attack works even when the identity of the malicious nodes is unknown and does not use any additional network bandwidth. The performance of a small multicast group will degrade seriously under these types of attacks even the solution is available. The proposed algorithm provides protection against black hole attack in MANET.

Sujatha et al. [9] proposed Design of Genetic Algorithm based IDS for MANET. In this work a technique to analyze the exposure to attacks in AODV, specifically the most common network layer hazard, Black Hole attack and to develop a specification based Intrusion Detection System (IDS) using Genetic Algorithm approach. The proposed system is based on Genetic Algorithm, which analyzes the behaviors of every node and provides details about the attack.Genetic Algorithm Control (GAC) is a set of various rules based on the vital features of AODV such as Request Forwarding Rate, Reply Receive Rate and so on.

Konate et al [10] proposed an Attacks Analysis in mobile ad hoc networks: Modeling and Simulation. In this paper present work is dedicated to study attacks and countermeasures in MANET. After a short introduction to what MANETs are and network security we present a survey of various attacks in MANETs pertaining to fail routing protocols. We also present the different tools used by these attacks and the mechanisms used by the secured routing protocols to counter them. In this defined the concept of DoS like its various types. They presented several alternatives of DoS attacks met in MANETs, their operating process thus the mechanisms used and the protocols which implement them to counter these attacks.

Gandhewar et al [11] proposed Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network. This work mainly focuses on sinkhole problem, its consequences & presents mechanism for detection & prevention of it on the context of AODV protocol. Sinkhole is one of severe kind of attack which attempts to attract most of network traffic towards it & degrade the performance of network. AODV is mainly analyzed under blakhole, wormhole & flooding attack, which needs to analyze under other kinds of attack also. It also shows performance of AODV with no sinkhole attack, under attack & after applying our mechanism in the form of simulation result obtained for certain variation of nodes in network, by considering performance metrics as throughput, PDR, End to end delay & Packet loss.

Sharma et al [12] proposed An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET. In this work a solution to the black hole attack in one of the most prominent routing algorithm, ad-hoc on demand distance vector (AODV) routing, for the MANETs. The black hole attack is one of such security risks. In this attack, a malicious node falsely advertise shortest path to the destination node with an intension to disrupt the communication. The proposed method uses promiscuous mode to detect malicious node (black hole) and propagates the information of malicious node to all the other nodes in the network.

VI. CONCLUSION

Mobile Ad Hoc Networks have the ability to setup networks in a cruel environment where it may not possible to deploy a traditional network infrastructure. Whether ad hoc networks have vast potential, still there are many challenges left to overcome. Security is an important feature for deployment of MANET. Security is such an important feature that it could determine the success and wide deployment of MANET. A variety of attacks have been identified. Existing security techniques can be applied within wireless networks to diminish security threats. As an advantage, the decentralized nature of MANETs provides additional robustness against the single points of failure. The wormhole attack is a type of attack that performs the malicious activity by creating own link and avoids actual link i.e. the actual path for data delivery.

VII. EXCEPTATION OUT COME

we proposed detection as well as prevention technique against wormhole attack, for detection we use profile base detection technique and get attacker node information like node number, number of attack packet, attack time etc. after that we prevent wormhole attack using neighbor trust worthy base technique and secure the MANET communication, through our proposal we provide secure as well as reliable communication and simulate through network simulator-2 and analyze the network behavior in attack and prevention case. After that we measure the performance of network on the bases of network parameter like throughput, packet delivery ratio, throughput, routing load etc.

REFERENCE

[1] Pallavi Sharma, Prof. Aditya Trivedi "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", 3rd IEEE International Conference on Communication Software and Networks (ICCSN), pp. 307 – 311, 2011.

[2] S. Yi and R. Kravets, "Composite Key Management for Ad Hoc Networks". Proceedings of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services(MobiQuitous'04), pp. 52-61, 2004.

[3] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Low Price Edition, Pearson Education, pp. 521, 2007. Dokurer, Semih."Simulation of Black hole attack in wireless Ad-hoc networks". Master's thesis, AtılımUniversity, September 2006.

[4] Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou. "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks", Journal of Internet Engineering,Vol.- 2, no.1, 2008.

[5] Husain. Shahnawaz, Gupta S.C., Chand Mukesh "Denial of Service Attack in AODV & Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Adhoc Network*",* International Conference on Computer & Communication Technology (ICCCT-2011), pp. 292- 297, 2011.

[6] Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, Ting-Yun Chi, Sanjay K. Dhurandher "Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks", proceedings of IEEE Global Telecommunications Conference (GLOBECOM 2011), pp. 1-5, 2011.

[7] Dr. N. Sreenath, A. Amuthan, & P. Selvigirija "Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs", International Conference on Computer Communication and Informatics (*ICCCI* -2012), pp. 1-7, 2012.

[8] K. S. Sujatha, Vydeki Dharmar, R. S. Bhuvaneswaran "Design of Genetic Algorithm based IDS for MANET", International Conference on Recent Trends in Information Technology (ICRTIT), pp. 28-33, 2012.

[9] Dr Karim KONATE, GAYE Abdourahime "Attacks Analysis in mobile ad hoc networks: Modeling and Simulation", 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, pp. 367 – 372, 2011.

[10] Gandhewar, N., Patel, R. "Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network", Fourth International Conference on Computational Intelligence and Communication Networks (CICN), pp. 714 – 718, 2012.

[11] Singh P.K. Sharma, G. "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 902 – 906, 2012.