Disclosure of Malevolent in MANET: A Survey

Ms. K. Sindhu[1] Mrs. S. Dhanalakshmi[2] Dr. S. Karthik[3]
[1]P.G. Student [2]Associate Professor [3]Dean
[1,2,3]Department of Computer Science & Engineering
[1,2,3]SNS College of Technology, Coimbatore, India

Abstract— *MANET is a wireless network technique, having features like dynamic topology and own-configuring ability of nodes. The self-configuring ability of nodes in MANET made it popular among the critical situation such as military use and emergency recovery. In MANET there no infrastructure hence each node plays as a host and router. Here all the users connected to each other by P2P network. Decentralized defines there is nothing like client and server. All nodes in network is acted like a source and a destination. Due to the dynamic nature of mobile Ad-HOC network it is more vulnerable to attack. We have many types of attacks in network the major security problems in ad hoc networks called the black hole and gray hole problem. It occurs when a malicious node referred as black and gray hole joins the network. So to protect MANET from many attacks, it is important to develop an efficient and secure system for MANET. In this article we discus different types of methods and techniques to detect and prevent attacks in mobile ad- hoc networks.*

Keywords— Mobile Ad hoc Network, Malicious, Security Issues in MANET

I. INTRODUCTION

In most enterprise environments security today is based on the approach of defense-in-depth, where multiple layers of defenses are used to prevent adversaries. This approach is based on the premise that, even if an adversary penetrates one of the layers of defense, he will not be able to cause much harm because the other layers will provide an adequate level of protection. The major advantage of a wireless network is the potential of the node to communicate with another node present in the network, while changing their position. Basically there are two types of systems that have been implemented for wireless network. First, is the fixed infrastructure wireless model, this system consists of a number of mobile nodes and comparatively less, but more powerful base stations that remains fixed. These base nodes are wired using modems and landlines. The communication between a base node and a vehicle node takes place via the wireless medium within its range. This model needs a stable infrastructure. Second, is the Mobile Ad hoc Network (MANET), it has been introduced to overcome the problems associated with wired network and implemented only when it is required. The key technology in traditional wire line networks that is used as a first layer of defense at the perimeter of the network is firewall. Firewalls are used to prevent outsiders from penetrating the enterprise network. Cryptography techniques are another technology being used as a preventive layer to keep outsiders from accessing critical resources.

Mobile network has emerged as new methods to give anytime, anywhere transmission. Improvingly wireless ad hoc networks are being worked in the critical domain, emergency rescue and analysis missions, as well as civilian ad hoc places like rooms and meetings. This is due to the speed and easy in setting up such networks. Wireless ad hoc networks not similar functions from a wired network, such as public medium, dynamic topology, limited bandwidth and limited power. The use of mobile ad hoc networks in recent years has been widespread in many applications, added few tactical functions, and as like authorized has become one of the main techniques in MANETs

In this article we give a survey of techniques used to elaborate security systems in MANETs environment. Our literature of techniques to implement detection and prevent in MANETs is presented in section 2. And section 3contains conclusion of our article.

II. ROUTING IN MANET

The security of MANETs compromise with prevention and detection techniques to struggle individual disobeying nodes. With respect to the capability of these techniques becomes vulnerable when multiple malicious nodes conspire together to start a collaborative hacks, which can result to more shocking damages to the network. These networks are highly susceptible to routing hacks such as blackhole and grayhole.

There are mainly 4 types of routing protocols they are:

1) Proactive routing
2) Active again –routing (Re active)
3) Hybrid routing
4) Hierarchical routing

A. Proactive Routing

It is a table driven technology and it follows renewed lists of destinations and the routes by periodically dispensing routing tables through the whole network. The disadvantage of these algorithms is with respective amount of data for maintenance alike slow acknowledgement on replacement and failures. Proactive algorithms are such as Optimized Link State Routing Protocol (OLSR), and Destination Flow Distance Vector (DSDV).

B. Reactive Routing

It is an On-demand routing topology it finds the route on appeal by overflow the network with Route Request packets. The disadvantage of these technologies will take high time in finding route, unwanted flooding which can lead to network blockage. Ad hoc routing examples are On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR).

C. Hybrid Routing

It is the merged of both proactive and reactive routing. The routing is mainly identify with the proactively examined routes and then aids the demand from furthermore starting point nodes over reactive flooding. The optimum of one or the other technology needs prearrangement for expected cases. The disadvantage of these algorithms is it focused on

number of additional nodes started the response to traffic flow demand depends on ramp of traffic volume. Examples of hybrid technologies are ZRP (Zone Routing Protocol).

D. Hierarchical Routing

In this protocol the choice of proactive and reactive routing is not a independent on the level in which the node is present. The routing process is primarily recognized with some proactively analyzed routes and then aids the demand from furthermore activated nodes over reactive flooding on the lesser levels. The dis-advantages of this technology is that it depends on complexity of nesting and addressing system and response to traffic requital depends on interlocking limits. Examples of hierarchical routing are: CBRP (Cluster Based Routing Protocols), FSR (it's based on Fisheye State Routing protocols)

E. Attacks in MANET

1) Black Hole

A black hole node exploits a routing protocol. In black hole hack, the attacker node may or may not be authorized in the network i.e. it may be owned in some other network. When the attacker node receives a route request packet (RREQ) from a neighboring node it not a quick access to sends route reply (RREP) as having a perfect route and a shortest path to the required destination even though the route is not a true thus creating confusion. In this way the attacker node attacks all the route requests.

2) Gray Hole

A Gray hole hack is tougher to detect because nodes can drop packets partially due to its malicious nature or due to overload, profusions and selfish nature of the nodes which are involved in the routing process.

3) Wormhole Attack

The most powerful attack now a day's present in the ad hoc network is wormhole attack. This type of attack requires the collaboration of two attacker nodes that take part in the ad hoc network.

4) Denial of Service

Another type of attack is denial of service, which focus to capture the availability of a particular node or even the functions of the whole ad hoc networks. In the simple wired network, the DoS attacks are performed by inserting some specific network traffic to the goal node so as to consumes the energy of the node and make the services provided by that particular node become unavailable.

F. Techniques for Detection of Attacks

In this section we give a survey on attack detection for MANETs. Mainly, we will present essentially the well-known techniques used for security according to the recent literature. Here we discus about many types of proposed technique for detecting attacker in mobile ad-hoc networks, detailed literature survey is below.

III. LITERATURE SURVEY

A. CBDS Based on Hybrid Defense Architecture

CBDS which integrates the proactive and reactive defense architectures, and randomly cooperates with a problematic neighbor node. By using the location of the adjacent node as the bait destination address, it baits attacker nodes to reply RREP and find the attacker nodes by the proposed reverse tracing program. Finally the found attacker node is tabled in the attacker node table and check all other nodes in the network to stop any communication with them. As a solution our technique can decrease data loss that cause by the malicious nodes and have better packet delivery ratio.

B. Dynamic Source Routing

This paper describes the design and performance of a routing protocol for ad hoc domain that alternatively uses dynamic source routing of packets between hosts that want to communicate. Source routing is a routing method in which the client of a data determines the complete sequence of nodes through which to forward the data; the client clearly account this route in the packet' s header, identifying each forwarding "hop" by the location of the future node to which to share the data on its way to the destination host.

C. Mobile-Backbone Protocol

Concentrate on protocols governing the operation of the MBN's Bnet and Anets. The MBN is designed so that it involves a sufficient hut not excessive number of backbone nodes (minimality feature), while providing high coverage. so that high fraction of the low power nodes can access at least a single Backbone Node (BN) through a path of at most hops. The MBN should also implement a survivable in robust topology, such as that realized by a k-connected backbone network.

D. Eliminating Black hole and Cooperative Black hole

In this article and after having detailed how a black hole attack is handling, a solution consisting in checking the good forwarding of the traffic by an center node, was proposed. The result is based on the well-known principle which is the Merkle tree A Merkle tree is a binary tree in which, all leaf cares a given value and the value of an interior node (including the root) is a single-way key process of the node's children values.

E. Mitigating Routing Misbehavior

Here explore different techniques to detect and mitigate routing misbehavior. In this way, we can make only minimal differences to the underlying routing technique. We introduce two extensions to the Dynamic Source Routing algorithm (DSR) to checking the effects of routing malicious: the watchdog and the path rater. The watchdog identifies misbehaving nodes, while the route rater omits routing data over these nodes. When a node forwards a packet, the node's watchdog checks that the future node in the path also sends the packet. The watchdog does this by listening promiscuously to the other node's communications. If the future node does not forward the packet, then it is misbehaving. The path rater uses this intelligence of attacker nodes to select the network path that is most likely to deliver packets.

F. Detection and Removal of Cooperative Black/Gray hole

We present a mechanism to detect and remove the above two types of malicious nodes. Our technique works as follows. First a backbone network of trusted nodes is established over the ad hoc domain. The sender node continuously requests one of the backbone nodes for a restricted (unused) IP address. Whenever the node needs to

make a communication, it not only sends a RREQ in search of destination node but also in search of the unauthorized IP randomly. As the Black/Gray holes send RREP for any RREQ, it replies with RREP for the Restricted IP also. If any of the path cooperates positively with a RREP to any of the unauthorized IP then the source node starts the finding process for these attacker nodes.

G. Detection of Routing Misbehavior

In this article, used a novel technique called 2ACK which provides an add-on technique for routing schemes that finds the routing malicious and to overcomes their adverse effect. The main feature of 2ACK is to forward two-hop ack data in the against direction of the routing path and to reduce additional routing overhead. The process of the technique was checked and simulated and 95% packet delivery ratio was achieved when 40% misbehaving nodes were present in the MANETs. When a node forwards a data packet successfully over the next hop, the receiver node of the neighbor node link forward return a special two-hop ack named as 2ACK indicating the successful data packet transmission.

H. Prevention of Cooperative Black Hole Attack

In this article, we develop a methodology to checking many blackhole nodes adjusting as a group. The method works with little modified AODV protocol and makes use of the Data Routing message table in adding to the temporary and current routing tables. A black hole has more than one feasibility. First, the node uses the ad hoc routing algorithm, such as AODV, to advertise itself as having a authorized path to a receiver node, even though the path is phony, with the motivation of intercepting packets. Next, the node consumes the intercepted data.

I. REAct: Resource-Efficient Accountability

We investigate the complexity of uniquely checking the set of attacker nodes who refuse to forward packets. We propose a novel attacker checking scheme named REAct that provides ability-effective computability for node attacker. REAct checking attacker nodes based on a series of desequence audits triggered upon a behaviour drop. We show that a sender-receiver pair using REAct can check any number of freedom attacking nodes based on performance proofs gave by nodes. Proofs are built using Bloom filters which are storage-efficient membership structures, thus particularly decreases the communication overhead for misbehavior detection.

J. Providing Fault-Tolerant Ad hoc Routing

Here, a new routing service named best-effort fault- tolerant routing (BFTR). The design goal of BFTR is to provide packet routing method with more delivery ratio and less overhead in presence of misbehaving nodes. Instead of judging whether a route is best or worst, i.e., whether it having any attacker node, BFTR evaluates the routing feasibility of a path by its end-to-end performance, by continuously observing the routing performance, BFTR dynamically routes packets via the best scalable path. BFTR gives an effective and uniform result for a broad range of node misbehaviors with very some security assumptions. The BFTR method is using over both analysis and extensive simulations. The results mention that BFTR best develop the ad hoc routing performance in the presence of attacking nodes.

K. Defending against Collaborative Packet Drop Attacks

Here mention a new technique for audit based detection of collaborative packet drop attacks. We first study the vulnerability of the REAct system and illustrate that collaborative adversaries can compromise the attacker identification procedure by sharing Bloom filters of packets among them. In the new approach, a collaborative attacker cannot generate its node performance proofs if an innocent node before it does not get the data sets clearly. The new approach will permit the method to successfully address the routing part in which packet drop attacks are conducted. We also investigate the security of the our method and model techniques to further decrease the overhead on the intermediate nodes.

L. Black Hole Attacks in Mobile Ad Hoc Networks

The major process of this work is threefold. First, we implement the simulation of the solutions proposed for the cooperative black hole attacks by Ramaswamy et al. Second, we also add some changes to the algorithm to improve the accuracy in preventing black hole attacks. In this paper we completely describe the implementation details which here locate the various problems which are not mentioned in. Finally, we compare the performance of the modified solution with other previous results in terms of throughput, end-to-end delay route request overhead, and packet lost percentage.

IV. CONCLUSION

Ad hoc networks are an increasingly and promising area of research with lots of practical applications. However, MANETs are vulnerable to attacks, due to their dynamically changing topology, absence of centralized infrastructures and open medium of communication. Due to this vulnerability, detection prevention methods such as authentication and encryption are not able to eliminate the attacks, it only reduces the attacks. In this paper a survey on different existing techniques for detection of attacks in MANETs with their defects is presented. The detection techniques which construct exploit of proactive routing mechanism have best data delivery rate and correct detection probability, but have higher overheads. As the transposition security model is applied to the cooperative bait detection approach the data is forward in a secured process and the data delivery rate is also improved and the loss of data packets is decreased.

REFERENCES

[1] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," inProc. 2nd Intl. Conf. Wireless Commun.,VITAE, Chennai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

[2] S. Corson and J. Macker, RFC 2501," Mobile Ad hoc Networking(MANET): Routing Protocol Performance

Issues and Evaluation Considerations," Jan. 1999. (Last retrievedMarch18,2013).

[3] C. Chang, Y. Wang, and H. Chao, "An efficient Mesh-based core multicast routing protocol on MANETs,"J. Internet Technol., vol. 8, no. 2, pp. 229–239, Apr. 2007.

[4] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., pp. 153–181, 1996.

[5] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: Amobile-backbone protocol for ad hoc wireless networks," inProc. IEEEAerosp. Conf., 2002, vol. 6, pp. 2727–2740.

[6] A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperativeblackhole attacks in wireless ad hoc networks,"Intl. J. Comput. Sci. Inf.Security, vol. 7, no. 1, 2010.

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," inProc. 6th Annu. 2000, pp. 255–265.

[8] K. Vishnu and A. J Paul, "Detection and removal of cooperativeblack/gray hole attack in mobile ad hoc networks,"Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.

[9] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior inMANETs,"IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550,May 2007.

[10] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.

[11] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard,"Prevention of cooperative blackhole attacks in wireless ad hoc networks," inProc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.

[12] H. Weerasinghe and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," inProc. IEEE ICC, 2007, pp. 362–367.

[13] Y. Xue and K. Nahrstedt, "Providing fault- tolerant ad hoc routing service in adversarial environments," Wireless Pers.Commun., vol. 29, pp.367–388, 2004.

[14] W. Kozma and L. Lazos, "REAct: resource- efficient accountability fornode misbehavior in ad hoc networks based on random audits," inProc.WiSec, 2009, pp. 103–110.

[15] W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," inProc.28thIEEE Int. Symp.Reliable Distrib. Syst., New Delhi, India, Sep.2009.

[16] IEEE Standard for Information Technology, IEEE Std 802.11-14997, 1997, "Telecommunications and Information exchange between systems: wireless LAN medium access control (MAC) and physical layer (PHY) Specifications", pp. i-445.