Available at: www.researchpublications.org

Technical Analysis of Intrusion Detection in Routing Protocol for Mobile Ad Hoc Network

S.V.Shirbhate
Research scholar, Amravati
san_shirbhate@yahoo.co.in

Dr. S.S.Sherekar
S.G.B.A.U Amravati
ss_sherekar@rediffmail.com

Dr. V.M.Thakare
S.G.B.A.U Amravati
vilthakare@yahoo.co.in

Abstract- Mobile computing environment are vulnerable to malicious attacks ranging from passive eavesdropping to an active interfering. In wireless network attacks can come from all the directions and target at any node. Compensation can include leaking secret information, message corruption and node masquerade. In mobile ad hoc networks security is hard due to the dynamic nature of the relationships between the participating nodes as well as the vulnerabilities and limitations of the wireless transmissions medium. In order to avoid such circumstance, there is need to develop new architecture and mechanisms to protect the wireless networks and mobile computing applications. All nodes in MANET must function as routers that discover and maintain routes to other nodes in the network. Due to MANET's characteristics, it is a complicated job for IDS to detect routing attacks. Intrusion detection system plays an imperative role in network environment for security. Routing attacks may be launched by the malicious node since node acts as a router in multi hopping.

This paper focuses on various vulnerabilities in routing protocol and security methods and analyzes various parameters which plays important role in order to increase the throughput.

Keywords- Intrusion Detection System, MANET, Mobile Computing.

I. INTRODUCTION

Now a day constructing flexible and improvisational nature of wireless network is advantageous for many applications such as military or civilian scenarios concerning security problem due to its characteristics. Initially wireless network is classified into two types: infrastructure based network and ad hoc network [1][2]. Infrastructure based wireless network consist of laptops and mobile phones using IEEE standard 802.11 in which all nodes access external world using fixed access point. The wireless communication among nodes and the access point enables the mobility of the node if required [3]. However wireless access to the service providing infrastructure is limited to particular areas. Also buildings and physical obstructions further restrict availability [4]. In ad hoc network without any infrastructure all nodes are communicating with each other. MANET is a special kind of ad hoc network. Mobile ad hoc network has a tremendous popularity in the domain of networking. Mobile ad hoc network is a collection of wireless nodes. It can be rapidly deployed as a multi hop packet radio network without the aid of any existing network infrastructure or centralized administration. Nodes within each other's radio range communicate directly via wireless links [3]. MANET is highly vulnerable to different type of attack due to its characteristics [2]. As the expansion in wireless devices, the use of distributed method with secure requirement is also increases. In this situation trust is introduce to measure the trustworthiness of node to participate in any expected operation. However security mechanism involving trusted third parties may no longer be viable in mobile ad hoc networks [5]. So development of more reliable security mechanism is needed. Before the development of any security measure to secure mobile ad hoc network it is important to study various vulnerabilities and security approaches.

The remainder of the paper is organized as follows, section II elaborates on the vulnerabilities in routing protocol, section III describes the security approach in routing protocol and section IV contains analysis and discussion. Finally at the section V conclude by discussing the outcome of study.

II . VULNERABILITIES IN ROUTING PROTOCOL

Although MANET is popular among the critical applications, its characteristics are more vulnerable to attacks. There are two levels of attack in MANET; attacks against basic mechanism and attacks against the security mechanisms. The mobile ad hoc networks have their own unique mechanism such as the use of wireless links for communications, employing routing strategies and operate in a distributed manner.

In mobile network each mobile node acts as a router and forwards the packets for other peer nodes. Routing is one of the fundamental mechanisms in the ad hoc networks. Improper and insecure routing mechanism degrades the network performance and also such type of network vulnerable to many security attacks. Because of nodes lack of physical protection, malicious attacker can easily imprison and compromise node to achieve attacks. Most of the routing protocols

such as AODV, DSR, and wireless MAC protocols such as 8002.11 assume that every node in network behaves cooperatively and trustworthy with other nodes[4][6]. However malicious attacker can readily become router and disrupt network operations by purposely violating the protocol specifications [6] [7].

The MANET protocols are facing different routing attacks such as flooding, black hole, link spoofing, replay, wormhole [7]. Responding to many security attacks against mobile ad hoc network basic mechanisms, researchers have introduced a number of security measures to protect the networks. But all these security measures also vulnerable to attacks for example attacks against security mechanisms are stealing username and password to get unauthorized access in the network.

Attack against the mobile ad hoc network may vary depends on environment, communication layer and level of mobile ad hoc network mechanisms are targeted. In designing any security measure for mobile ad hoc network, it is needs to consider several attacks characteristics. Here focusing on the vulnerabilities of mobile ad hoc network against routing protocol are considered. Some of the common attacks that could be launched against mobile ad hoc network routing protocols are following illustrate.

A. Black Hole Attack

In this attack, malicious nodes trap all the neighboring nodes to attract all the routing packets to them. Malicious nodes can launch the black hole attack by advertising to the neighboring nodes as having the most optimal route to the requested destination i.e. malicious node impersonates a destination node by sending fake route replay RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node [8]. In this attack, only one attacker is involved and threatens all its neighboring nodes.

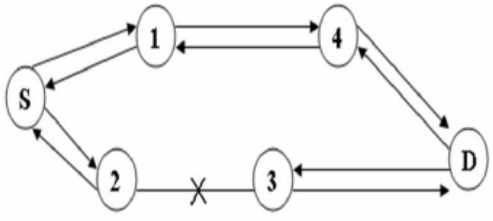

Fig 1. Black hole Attack

It means that when node transmits any type of routing control packet i.e. RREQ, RREP, RERR, it increases its sequence number [9]. So to detect this attack, destination sequence number is taken into account.

B. Resource Consumption Attack

Malicious node attempt to consume both network and resource by generating route reply packets to source send unnecessary packets to block the route. The resources that are targeted are battery power, bandwidth, and computational power, which are only limitedly available in ad hoc wireless networks. The attacks could be in the form of unnecessary requests for routes, very frequent generation of beacon packets, or forwarding of stale packets to nodes. Using up the battery power of another node by keeping that node always busy by continuously pumping packets to that node is known as a sleep deprivation attack [8].

C. Packet dropping Attack

Routing messages can be interrupted by this attack. In this attack an adversary collaborates as usual in the route discovery process and launches the constant packet dropping attack. Instead of constantly dropping all the packets, adversaries may vary the technique using random, selective or periodic packet dropping attacks in order to help the interrupting behavior remain buried. The node conserves its energy and resources by acting selfishly but it may also cause many network problems such as segmentation [9].

III. SECURITY APPROACHES IN ROUTING

As a security point of view, the MANET provides security services such as authentication, confidentiality, integrity, anonymity and availability to the mobile users. From the security design perspective MANET have no clear line of defense [7]. Successful implementation of MANET depends on user's confidence in its security. The security research in MANET has focused on key management, routing protocols and intrusion detection techniques [7] [9]. Encryption and authentication as intrusion prevention are not sufficient. However these techniques have limitations on the effect of prevention techniques in general and they are designed for set of known attacks [10]. Main drawback of this approach is that it introduces a heavy traffic load to exchange and verify keys which is very expensive in terms of bandwidth constraint for MANET nodes with limited battery and limited computational capability [7].

Secure ad hoc routing protocol has been proposed as a technique to enhance the security in MANET. [6] Proposed a novel IDS named as Enhanced Adaptive ACKnowledgement (EAACK) protocol specifically designed for MANET and compared it against other popular mechanisms in different scenarios through simulation.

[4] Propose a combination of secure routing protocol and IDS for strengthening the defense of MANET. Several security solutions that have been proposed to secure the routing protocol. IDS must be efficient if its solutions are efficient in terms of various parameters such as communication overhead, energy consumption and computationally affordable by a portable device. Hence the following session elaborates the various techniques,

parameters used for detecting attacks. Depending on the attack various parameters are used in order to increase the throughput.

IV. ANALYSIS AND DISCUSSION

The following table [1] analyzes performance of intrusion detection techniques against routing attacks.

Table 1: Performance Analysis of Intrusion Detection Techniques Against Routing Attacks

Author name	Year of pub.	Input	Technique	Attacks	Results	Advantages	Limitations	Performance
Anand Patwardhan et al.	2005	Packet traffic	Combined secure routing protocol and IDS	Secure routing protocol detect Routing disruption attack, rushing attack & IDS detects high level mangling attack and grey hole attack, DoS	1. Drop rate for IDS 2. Acceptance rate for resource consumption attack. 3.Reachability and response time	**1**.Collaborative IDS offers a collective response to misbehaving nodes. **2**.IDS work on thresholds as well as signal strength which help to determine node is misbehaving or simply moved out of range. **3**. It also help in selection of node to monitor , increase the scalability and detection accuracy of IDS	Due to signature verification during the route maintenance at each node the response time indicates delay in packet traversal time	Packet loss is not significantly affected by additionally overhead of signature verification during route maintenance whereas response time indicate delay in packet traversal time.
R.saminathan et al.	2010	Network traffic data	Profile based neighbor monitoring and threshold based IDS (PROFIDES)	Packet drop attack And black hole attack	1.Traffic intensity 2. packet drop 3.No. of attacks and 4. mobility rate	**1**. Due to threshold, degradation behavior of system improved and brings the system back into normality. 2. PROFIDES works in highly dynamic varying environments where traffic intensity increases on mobility or in nodal activity. 3. It controls traffic intensity in setup as time increases by duly informing all other nodes about attacker.	Limited information in data packet profile is used to identify or recover the support.	Compared to AODV protocol, PROFIDES detection rate is better and detection is faster whereas in AODV packet drop increases on increasing of traffic load due to mobility nodes.
Elhadi Shakshuki et al.	2011	Data packet	Acknowledgement based IDS (EAACK)	Packet dropping attack	Packet delivery ratio And routing overhead	1. It is designed to deal with false misbehavior, limited transmission power and receiver collision. 2. Due to digital signature, it prevents the attacker from forging acknowledgement packets.	1. Suppose source node and destination node are malicious then all acknowledgement packets are digitally signed by sender and verified its receiver. 2. Due to digital signature, extra resources are required.	Comparative study shows the positive performance against watchdog, TWOACK, AACK in terms of receiver collision, limited transmission power and false misbehavior but due to digital signature in some scenarios routing overhead is more.
Farhan Abdel Fattah et.al	2010	Audit data	Conformal predictor K-Nearest Neighbor and Distance	1. Black hole 2. Resource consumption 3. Dropping	1.False positive rate 2.Detection rate	Due to combining the anomaly andsignature detection technique this method	Calculating the non conformity score is complex task.	Detection model using both CP-KNN and DOD achieves higher detection rate and decrease

			based outlier Detection	routing traffic	3.Detection Accuracy 4.Risk Index 5.Receiver Operating Characterstics	anomalies with low false positive rate, high detection rate and achieve higher detection accuracy.		the false positive rate than a using single classifier. The prediction accuracy of combined prediction modelis higher than the model using a single classifier.
Rakesh shrestha et al.	2010	Audit data contains local routing information, data & control information along with traffic statistics	Cross layer intrusion detection system in which data mining technique (fixed width clustering algorithm)	Anomalies 1. DoS attack 2. Sink hole	1. True positive 2. False positive rate	1. Due to combining cross layer features, attacks originating from any layer can be detected. 2. Due to the association module, overhead of data collection and learning minimized. i.e IDS consumes low energy by adopting association rule	Classification is based on threshold. So determining the threshold is monotonous task.	The cross layer technique incorporating leads to an escalating detection rate in the number of malicious behavior of nodes increasing true positive and reducing false positives.
Oleg Kachirski	2002	Audit data from multiple network sensor	Multi sensor IDS based on mobile agent	Anomaly detection	False alarm	1. It is lightweight, low overhead mechanism. 2. This approach minimizing the cost of network monitoring and maintaining monolithic IDS system which resulting greater availability of computational resources.	The election of monitoring node is a complex task.	Decreasing the level of monitoring can resulting the greater availability of computational resources of entire network.
Baolin Sun et al.	2005	Audit every RREQ, RREP and RERR in AODV packet	Specification based Intrusion detection technique	Routing disruption attack	Control overhead, delivery ratio, percentage ofRR EP forwarded	In specification based ID approach, correct behavior of critically objected are manually abstracted and crafted as security specification. So here intrusions can be detected without exact knowledge about them.	1. Developing specification is time consuming. 2. Many complex attacks do not violate the specification directly and cannot detected using this approach.	Comparison between AODV and SAODV shows that, SAODV increases overhead, but average delivery ratio less than AODV due to overhead. When attackers exist, packet drop ratio is less in SAODV i.e. attackers are less effective against SAODV

Although the security providing in routing protocol, the role of routing of routing protocol is just to create and maintain routers. SecAODV protecting the network from routing disruption attack by using signed control messages, but still it is possible for attackers to selectively drop only data packets. So IDS emphasizes the MANET by detecting attacks such as grey hole and DoS. In this approach delay in packet traversal time due to signature verification in route maintain at each node. IDS should be scalable for its effectiveness but mobile devices can get overwhelmed quickly if it starts monitoring all packets in its neighborhood which requires large amount of data traffic in dense. Also monitoring node needs to have efficient data structure to monitor traffic efficiently. [4] System used threshold based approach for

temporary anomalous behavior due to congestion. In this approach each packet is buffered on neighbor node corresponding to the same packet being buffered by the monitoring node which causes the large amount of memory until they are timed out. In [6] digital signature method is used to ensure that all acknowledge packets are authentic. So extra resources i.e. DSA and RSA digital signature scheme is used in this approach. The major concern of analysis is to evaluate performance of intrusion detection techniques against routing attacks.

V. CONCLUSION

This paper focuses on routing attacks against the mobile ad hoc network which may vary depending on environment, level of mobile ad hoc network mechanism such as attacks against basic mechanism and attacks against the security mechanisms. In designing any security measures for mobile ad hoc network, it is needed to consider various characteristics of attack. However since this study is focusing on the vulnerabilities of mobile ad hoc networks routing protocol, here some of the common attacks that could be launched against mobile ad hoc network are discussed. The common attacks such as Black hole, resource consumption, and packet dropping attacks against the MANET are actually launched by exploiting the routing messages. There is several security solutions have been proposed to protecting, detecting and responding attacks against the routing messages. However these methods have some limitations. So it is necessary to consider the various parameters while designing the effective IDS. Hence there is need to develop a scalable IDS architecture in future to collect sufficient evidences to detect attacks effectively.

REFERENCES

[1]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine 0163-6804/02, PP.70-75. October 2002.

[2]. Hadi Otrok, Joey Paquet, Mourad Debbabi and Prabir Bhattacharya, "Testing Intrusion Detection System In MANET: A Comprehensive Study", Fifth Annual Conference On Communication Networks and Services Research (CNSR'07), 0-7695-2835-X/07, IEEE Computer Society, 2007.

[3]. S. P. Manikandan, Dr. R. Manimegalai, "Evaluation of Intrusion Detection Algorithms for Interoperability Gateways in Ad Hoc Networks", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 9, ISSN: 0975-3397, PP.3243-3249, 2011.

[4]. Anand Patwardhan, Michaela Iorga, "Secure Routing and Intrusion Detection in Ad Hoc Networks", in the Proceedings of the 3rd International Conference on Pervasive Computing and Communications (PerCom), Kauai Island, Hawaii, PP.1-9.2005.

[5]. Po-Wah Yau and Chris J Mitchell, "Security Vulnerabilities in Ad Hoc Networks", the work reported in this paper formed part of networks and services area core 2 research program of the virtual center of excellence in mobile and personal communications, mobile VCE, 2004.

[6]. Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami, "EAACK – A Secure Intrusion Detection System for MANETs", This work was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Research and Graduate Studies of Acadia University, Copyright (c) 2011 IEEE ,PP.1-11, 2012.

[7]. S.Kannan, T.Kalaikumaran, S.Karthik and V.P.Arunachalm, "A Study on Various Attack Detection Methods in Mobile Ad-Hoc Networks", International Journal of Signal System Control and Engineering Application 3(3) ISSN: 1997-5422 published in Medwell Journals, pp. 34-39, 2010.

[8]. S.V.Shirbhate, Dr V. M. Thakare, Dr S.S.Sherekar**,** **"**Security Threats In Mobile Ad Hoc Network", proceeding of National Conferences on ITCCE, PP. 69-74, Feb 2012.

[9]. Farhan Abdel-FattahZulkhairi Md. DahalinShaidah Jusoh, "Dynamic Intrusion Detection Method for Mobile Ad Hoc Network Using CPDOD Algorithm", IJCA Special Issue on "Mobile Ad-hoc Networks MANETs", pp. 23-29, 2010.

[10]. S.Mangai, A. Tamilarasi, " An Improved Location aided Cluster Based Routing Protocol with Intrusion Detection System In Mobile Ad Hoc Network", Journal of Computer Science 7(4), ISSN 1549-3636, PP. 505-511,2011.

[11]. R. Saminathan, Dr. K. Selvakumar, "PROFIDES - Profile based Intrusion Detection Approach Using Traffic Behavior over Mobile Ad Hoc Network", International Journal of Computer Applications 0975 – 8887 Volume 7– No.14, October 2010.

[12]. Oleg Kachirski and Ratan Guha, "Intrusion detection using mobile agents in wireless ad hoc networks", In Proceedings of the IEEE Workshop on Knowledge Media Networking, pages 153–, Washington, DC, USAIEEE Computer Society, 2002.

[13]. Baolin Sun, Hua Chen,Layuan Li, "An Intrusion Detection System for AODV ", Proceedings of the 10th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS'05),0-7695-2284-X/05 , IEEE, 2005.