International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Intrusion Detection Techniques with Their Security Mechanisms for Mobile Ad Hoc Networks

Mr. Naveed Zishan, Ashwini Meshram

Department of Computer Science and Engineering, GHRAET, Nagpur, Maharashtra-440009, India

Professor, Department of Computer Science and Engineering, GHRAET, Nagpur, Maharashtra-440009, India

Abstract: ***Mobile ad hoc networks (MANETs) have emerged as a tremendous wireless networking technology. MANETs are scalable and does not require a fixed architecture .nodes of the network plays the dual role as the transmitter and as the receiver. The self configuring ability has made MANETs useful in various applications such as military use and emergency recovery. Within the same communication range nodes communicate with each other directly .otherwise they rely on others for message passing. The open medium and the wide distribution of nodes made MANETs vulnerable to malicious attackers. As MANETs have limited resources so a technique should be applied that is efficient in finding intrusions and it should provide security simultaneously. Keeping in mind that network overhead and flooding of packets should not occur.***

Keywords: MANET Intrusion Detection System; Digital Signature; Malicious nodes; Misbehavior report; Acknowledgement

1. Introduction

Mobile Ad hoc Network (MANET) is a cluster of movable nodes having transmitting and receiving mechanism due to which nodes can have one to one communication with nearer nodes inside radio range and if nodes fall outside radio range then they rely on neighbor nodes for packet passing [1]. MANET structure may vary depending on its application from a small, static network that is highly power constrained to a large-scale, mobile, highly dynamic network[2][3]. Many industries are there that have distant control through wireless networks makes use of the ability of mobile network as nodes do maintain their locomotion[4][5]. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. Two nodes can interact with each other within a limit , if the distance between nodes are too much so nodes trust on others nodes to transfer packets There are two types of MANETs: closed and open[6][7][8].

In a closed MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search/rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. Some resources are consumed quickly as the nodes participate in the functions. Battery power is considered to be more importance in a mobile environment. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes and their behavior is termed selfishness or misbehavior. A selfish node may refuse to forward the data it received to save its own energy [8].

MANET has two types of network, namely single-hop and multi-hop [9]. In a single-hop network, nodes which fall within same radio range can interact easily, but where as in a multi-hop network, far nodes have to trust on intermediate nodes transmit The routers can have a free motion and perform its routing. However, the open medium of MANET is vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks[10]. Attackers can easily insert the malicious or incorporate nodes into the network to achieve attacks. Such misbehaving nodes need to be detected so that these nodes can be avoided by well behaved nodes. Many schemes and intrusion detection systems proposed to detect such nodes[11].

2. Literature Review

Noman and hadi[2] proposed a scheme to Divided the mobile ad hoc network into 1-hop clusters where each node belong to at least one cluster . The node division also prolongs the life time of MANETs as the nodes are energy limited. As MANETS have limited energy to each nodes and each cluster has a leader with most remaining resources. Here the leader acts as intrusion detector

Noman and Hadi [2] also proposed a leader election method in presence of selfish nodes As the leader election faces two major hurdles First ,without incentives for serving others, a node might behave selfishly by lying about its remaining resources and avoiding being elected second electing an optimal collection of leaders to minimize the overall resource consumption may incur a prohibitive performance overhead to overcome these two shortcomings a mechanism is used called Vickrey, Clarke,and Groves(VCG) .

Jie Liu [3] proposed a combined intrusion detection and biometric based continuous authentication in Mobile ad hoc network .In this approach multimodal biometrics are used for continuous authentication and intrusion detection is modeled as sensors to detect system security state.the author has formulated the whole system as a partially observed Markov decision process considering both system security requirement and resource constraints. There are certain authentication mechanism such as Passwords but passwords are simple and easy to use but difficult to distinguish an

authentication users from imposters because there on direct connection between the user and password .for tokens,it is subject to being lost. But on the contrary Biometrics has a direct connection with the identity of the user . one of the major drawbacks of the system is that the system becomes more complex with the continuous authentication and dynamic management is required .as the system requires ample resource but MANETs has limited resources

J.Munchester and M.Turk[4] proposed an authentication system which verifies a user during initial login. However for tactical MANETs in the hostile environment where chance of node capture are high ,it is important to verify the presence of the authentic user continuously during the lifetime of MANETs the frequency of applying authentication depends on the severity of the environment, system security requirements and resource constraints. But on the other hand the author used the mechanism of authentication only at the initial stage and not thought the lifetime of MANETS.

A.Ross and A.K . Jain[5] proposed a unimodal biometric technology but it has its own strength and weaknesses. for example,iris pattern is more accurate than voice identification , but getting a good image of the iris is difficult . signature is a widely accepted authentication method,but it still remains a question if it could acquire the same level accuracy as the other biometric technologies.

Buchegger and LeBoudec [12] proposed an extension to DSR protocol called CONFIDANT (Cooperation of Nodes, Fairness In Dynamic Ad-hoc Networks), which is similar to Watchdog and Pathrater. Each node observes the behaviors of neighbor nodes within its radio range and learns from them. This system also solves the problem of Watchdog and Pathrater such that misbehavior nodes are punished by not including them in routing and not helping them on forwarding packets. Moreover, when a node experiences a misbehaving node, it will send a warning message to other nodes in the network, defined as friends.

Patcha [13] proposed a method in which nodes are classified into trusted ond ordinary nodes. The nodes which are involved in initial network formation are called as trusted nodes. The nodes which are joining later in to the network are called as ordinary nodes. Here nodes keep watch on other node with the help of message passing . the major drawback of this approach is flooding of packets

Michiard[14] proposed a mechanism called CORE for node cooperation in mobile ad hoc network .It only provides positive acknowledgement about packet delivery, due to which flooding of packets does not occur. its drawback is that it provides only partial information.

Table 1: Summery of previously existing approaches

Sr. No.	Author name	Methodology Used	Advantages	Drawbacks
1.	Noman and hadi[2]	Divided the network into clusters and each cluster has a leader with most remaining resources Methodology used are :VICKREY,CLARKE AND GROVES(VCG)	Network division reduces resource consumption	Nodes with ample resources might avoid being elected as leader
2.	Jie Liu and F.Richard Yu,[3]	Biometric based continuous authentication and intrusion detection simultaneously	Security increases due to continuous authentication	The system becomes more complex with continuous authentication and more resources are required for the system but MANET has limited resources.
3.	J.Muncaster and M.Turk[4]	Proposed method of authentication at the initial login.	complexity reduces due to onetime authentication	In tactical environment the chance of node capture is more. For these type of situations continuous authentication is needed
4.	A.Rass and A.K.Jain [5]	Proposed a unimodal biometrics technology	Unimodals are advantageous in small applications .	unimodal biometrics have shortcommings in accuricies
5.	S. Buchegger[12]	Proposed a method called CONFIDENT which stands for	CONFIDANT provides overall status about packet delivery.	CONFIDANT allows positive as well as negative reports and hence causes flooding and denial of services.
6.	A. Patcha and A. Mishra [13]	Proposed a method which classifies as trusted and ordinary nodes	Node are given a privilege.	Additional packets increases the network overhead
7.	P. Michiardi and R. Molva[14]	Proposed a method called CORE that enforce node cooperation in mobile ad hoc network	Flooding does not occur in this method	Core provides only partial information about packet delivery

3. Conclusion

Mobile ad-hoc networks which stands for a type of mechanism that comprises of wireless communication network with dynamic topology, and nodes interact via packet passing without any fixed infrastructure. . In study, it is found that necessity of secure routing protocol is still a burning question. There is no general algorithm that suits well against the most commonly known attacks. However, in short, it can be said that the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET. The nodes of the network have limited energy ,so there were certain approaches to divide the network into clusters and each clusters should have a leader with most remaining resources .But nodes with most remaining resources many a times denies being elected or lies about their resources. There were certain approaches that used biometric based continue authentication and intrusion detection simultaneously but lead to complexity in the system and needs more resources. Still there were approaches to

provide positive as well as negative report for the delivery of packets but this approach leads to flooding so there is need for better intrusion detection system with best security mechanism

References

[1] Elhadi M. Shakshuki,Nan Kang, and tarek R Sheltami ,"EAACK-A Secure Intrusion Detection System For MANETs"IEEE Transactions on Industrial Electronics Vol. 60,no.3, MAR,2013.
[2] Noman Mohammed, Hadi Otrok,, ''Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE Transactions on Dependable And Secure computing , vol.8, no. 1, JANUARY –FEBRUARY 2011.
[3] Jie Liu, F. Richard Yu, "Optimal Combined Intrusion Detection and Biometric-Based Continuous Authentication in High Security Mobile Ad Hoc Networks", IEEE Transactions on Wireless Communication, vol.8, no. 2,FEBRUARY 2009
[4] J. Muncaster and M. Turk, "Continuous Multimodal Authentication Using Dynamic Bayesian Networks," in Proceedings of second Workshop on Multimodal User Authentication, ., Toulouse, France, May 2006.
[5] A. Ross and A. K. Jain, "Multimodal Biometrics: An Overview", in proceedings of 12th European Signal Processing Conference, (EUSIPCO), in Vienna, Austria, pp. 1221-1224, September 2004
[6] S.Marti,T.J.Giuli, k Lai, and M.Baker," Mitigationg Routing Misbehavior In Mobile Ad Hoc Networks",in proceedings of 6th Annual.International .Conference on .Mobile Computer .Network ,2000,pp. 255-256
[7] D. Djenouri, N.Badache ",Cross-Layer Approach To Detect Data Packet Dropper In Mobile Ad Hoc Networks" , IWSOS 2006, LNCS 4124, pp.-163-176, 2006.
[8] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proc.ACM Workshop Wireless Secur., 2002, pp. 1–10.
[9] N. Nasser and Y. Chen, "Enhanced Intrusion Detection Systems For Discovering Malicious Nodes In Mobile Ad Hoc Network",in Proceedings of IEEE International Conference on communications, Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159
[10] T.Anantvalee and J.Wu," A Survey on Intrusion Detection In Mobile Ad Hoc Networks", in proceedings of wireless /mobile security, pp 159-180. New York: springer-Verlag,2008.
[11] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks:Challenges, design principles, and technical approach," IEEE Transactions on Industrial Electronics, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.
[12] S.Buchegger and J.Y.L Boudec, "Performance Analysis of The Confidant Protocol(cooperation of nodes : fairness in dynamic ad hoc networks)," MOBIHOC'02,in proceedings of the third ACM International symposium on Mobile ad hoc networking & computing ,pp 226-236, 2002
[13] A.Patcha and A..Mishra, "Collaborative Security Architecture for Blackhole Attack Prevention in Mobile Ad Hoc Networks", in proceedings of Radio Wireless Conferece -2003, pp 75-78
[14] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks" in Proceedings of the conference on Communication and Multimedia Security 2002 ,September 26-27 ,pp 107-121.