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

Securing Manets with Ticket Granting for Acknowledgement Based Intrusion Detection

Reshma R[1], Sreerag B M[2]

[1]M.Tech Scholar, Nehru College of Engineering and Research Centre

[2]Assistant Professor, Nehru College of Engineering and Research Centre

Abstract: ***Mobile ad hoc networks (MANETs) can be defined as a collection of large number of mobile nodes that form temporary network. Dynamic nature and limited transmission range of MANETs leads to many security challenges. This itself emphasizes the importance of security and the need for an efficient intrusion detection system in MANETs. IDS is a great research area as the applications of MANETs are increasing into various fields. So, an efficient Intrusion Detection System is to be developed which provides the integrity, confidentiality, non-repudiation and authentication.Enhanced Adaptive Acknowledgment (EAACK) has been developed which consists of three parts, namely, ACK, Secure ACK (S-ACK), and Misbehaviour Report Authentication (MRA).Each module works according to ACK received and so for preserving integrity each ACK is being digitally signed using DSA. The system enhances its security by introducing Ticket Granting System(TGS).TGS approves sender's request by approving Tickets according to their privilege levels. Movement of each node is monitored by TGS and maintains Black list and White list of nodes. Tickets are granted by checking these lists and three modules of IDS works to find intruders so as to ensure security in the system.***

Keywords: MANETs**,** Ticket Granting System(TGS),Digital Signature(DSA),Intrusion Detection

1. Introduction

A mobile ad hoc network (MANET) is a temporary, self-organizing network of wireless mobile nodes without the support of any existing infrastructure. Its features like self organizing and independent infrastructures makes it a good choice for usages such as communication and information sharing in disaster recovery operation, smart buildings and military battlefields. MANETs allow all nodes to communicate with each other either directly or indirectly with the help of their neighbors and soa node can act as a transmitter as well as a receiver[3]. All the nodes within the same radio range communicate with each other or nodes depend on neighbors to transmit if destination node is out of their radio range. MANET is highly vulnerable to attacks because, node configuration in highly dynamic topology, routing, and maintenance are done on its own. Anyhow minimal configuration and quick deployment make MANET ready to be used in emergency circumstances. The Figure 1 represents the configuration of MANET by using different wireless devices. Any type of wireless devices within a transmission range can be connected easily and effectively. A source finds out the shortest path to send data to the particular destination without considering the nature of the wireless device.MANETs are advantageous in this aspect.

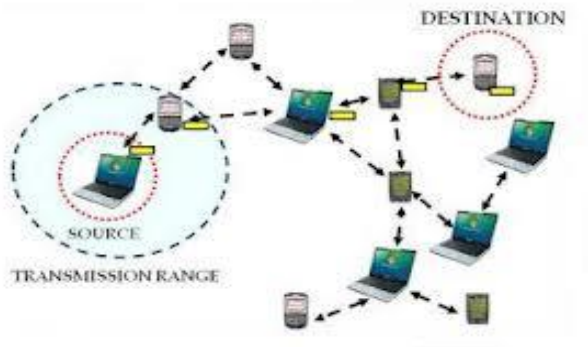

Figure 1: A Simple MANET Infrastructure

So there exists a possibility of attackers which can easily compromise MANETs by inserting malicious or non-cooperative node into the network. So, security is the important aspect in deploying MANET[2]. Many researchers are focusing in this specific area as there exists enormous number of security mechanisms. Due to MANET's distributed architecture and changing topology, a traditional monitoring technique or other security methods employed in strategic points like routers, switches are no longer feasible in MANETs. Intrusion detection system is to be designed specifically for MANETs which utilizes its properties and to reduce all its security challenges.

Intrusion Detection mainly aims to find out the malicious node using different approaches. Monitoring, neighbour based approaches are developed initially but no longer provide efficiency. This paper discusses Acknowledgement based IDS which is enhanced by Ticket Granting for data transfer. Acknowledgements are in-avoidable and so use them as intrusion detection parameter. Ticket granting ensures additional security an d authentication. The paper discusses the existing scenarios of IDS and then the system description with TGS. The security aspects are being checked without compromising network overhead, throughput and packet delivery ratio.

2. Related Work

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is an overall protection system that is installed either in a particular system or in every system. Researches in IDS have been started earlier itself and so describing and comparison of various approaches are difficult in this scenario. Thus most important and suitable in the situation are being discussed below.

Licensed Under Creative Commons Attribution CC BY

2.1. Watch Dog and PathRater

The Watchdog and Pathrater is a solution to the problem of selfish (or misbehaving) nodes in MANET. The system introduces two extensions to the DSR algorithm: the Watchdog, to detect the misbehaving nodes and the Pathrater, to respond to the intrusion by isolating the selfish node from the network operation. Watchdog improves the throughput of the network even in the presence of attackers. A counter is initiated if the next node fails to forward the data packet. When the counter value exceeds a predefined threshold, the node is marked as attacker. The Pathrater module uses the information generated by Watchdog to select a better route to deliver the packets, avoiding the selfish nodes. But the system fails in receiver and ambigious collisions, limited transmission power, false misbehaviorreport,partial dropping, and collusion.

2.2. TwoACK

TwoACK is being put forward after Watchdog mechanism inorder to overcome the receiver collision and limited transmitted power. Here intruder is found out by dividing the route into three nodes and acknowledgment of every data packet over three consecutive nodes is sent from source to destination. If ACK is not received in a predefined time, the other two nodes are marked malicious. The major drawbacks are Increased overhead, Limited battery power, Degrades the life span of entire network.

2.3 Dynamic Intrusion Detection

Dynamic Intrusion Detection is mainly used in large networks that uses clustering. This method is structured in more than two levels. Thus, nodes on first level are cluster heads, while nodes on the second level are leaf nodes. Here every node has the task to monitor, log, analyse. respond, and alert or report to cluster heads. The Cluster heads provides integration of data , computes intrusion and then filters the data. Overall security management is done by cluster heads.

2.4 Zone Based IDS (ZBIDS)

The adhoc network is spitted into non-overlapping zones. The nodes can be categorized into two types: the intrazone node and the inter-zone node (or a gateway node). Each node has an IDS agent run on it.Data collection module and detection engine, local aggregation and correlation (LACE) and global aggregation and correlation (GACE) are its components[3]. The data collection and the detection engine are responsible for storing audit data andanalyzing collected data. The LACE module is responsible for combining the results of these local detection engines and generating alarms if any abnormal behaviour is detected. These alarms are being broadcasted within the same zone. The GACE module, functions depends on the type of the node. If the node is an intra-zone node, it only sends the generated alarms to the inter-zone nodes. Thus, if the node is an inter-zone node, it receives alarms from other intra-zone nodes, aggregates and correlates those alarms with its own alarms, and then generates main alerts. The intrusion response module is responsible for handling the main alerts generated from the GACE.

2.5 AACK

Adaptive acknowledgement is the combination of TWOACK and ACK. Source sends packet to every node till it reaches the destination. Once reached, receiver sends an ACK in the reverse order. If ACK is not received within predefined interval, it switches to TWOACK scheme [4]. The major drawbacks is that it suffers from False misbehaviour report and Forged acknowledgment packets**.**

3. Literature Review

Enhanced Adaptive ACKnowledgement (EAACK) is a reinforced version of AACK which was proposed by N. Kang, E. Shakshuki and T. Sheltami.It is used to tackle false misbehavior, limited transmission power and receiver collision limitations of watchdog. It involves three parts namely ACK, SACK (Secure ACK), MRA (misbehavior report authentication)[1]. The overall scheme is based on ACK and so integrity is preserved.

3.1 ACK

ACK is the first way of sending data packets which is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehaviour is detected.

3.2 SACK

The S-ACK scheme is an improved version of the TWOACK scheme. Every three consecutive nodes work together to detect Misbehaving or malicious nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet[4] to the first node. In the presence of receiver collision or limited transmission power the method works well.

3.3 MRA

The MRA scheme is used to resolve the weakness of all other techniques[1]. Other IDS methods fails to detect misbehaving nodes with the presence of false misbehaviour report. The false misbehaviour report can be generated by malicious attackers to falsely report legitimate nodes as malicious. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. Another shortest route is being selected by the source and the data packet is send and the ID of the packet is compared with the last received packet at the destination. If the ID matches the report it is false misbehaviour report. False misbehaviour identification is the main aim of MRA module and it is not found in any other popular intrusion detection systems. EAACK have enhanced security due to the co-operative working of these three modules. This shows less overhead and maximum throughput with high packet delivery ratio.

Licensed Under Creative Commons Attribution CC BY

3.4 Digital Signature

EAACK scheme finds intruders based on the acknowledgement received. So it is essential to ensure integrity of all acknowledgement packets. Digital Signature Algorithm (DSA) is being used to sign all ACK packets. This preserves the exact sender being forged. RSA can also be used to provide signature but performance of DSA is far better than RSA [6].

4. System Description

MANETs are specifically designed to use for a particular scenario or purpose even then a system design should ensure the mandatory regulations such as integrity, non-repudiation, confidentiality, authentication and authorization. The mechanism that uses Adaptive Acknowledgement for intrusion detection was developed to provide all these regulations. But the system does not have any mechanism to store the details of the detected intruder. So that once an intruder is detected in a specific link it is known only to the source and it is not yet broad-casted to any node in the network.

4.1 Ticket Granting Server

A ticket granting Server is a stationary system that provides access rights to all other nodes within its transmission range. A node can send data packets to destination if and only if it have the ticket issued by the TGS. The whole network based on the scenario of application may require more than one TGS based on the transmission range. A single TGS leads to network and message overhead which in turn leads to centralized failure. Deploying static TGs is based on the application and transmission range. There should be a wired connection between various TGS so as to maintain an updated database which changes dynamically according to the varying behavior of nodes in the network[5]. A TGS issues tickets on the basis of behavior of nodes in the network. TGS stores the behavior of all nodes in the network in two lists namely White list and black List. TGS issues tickets for those nodes that request ticket for data transfer by comparing the black list. Ticket is not granted for black listed nodes. A node is black listed if it is reported as malicious for a predefined number of times.

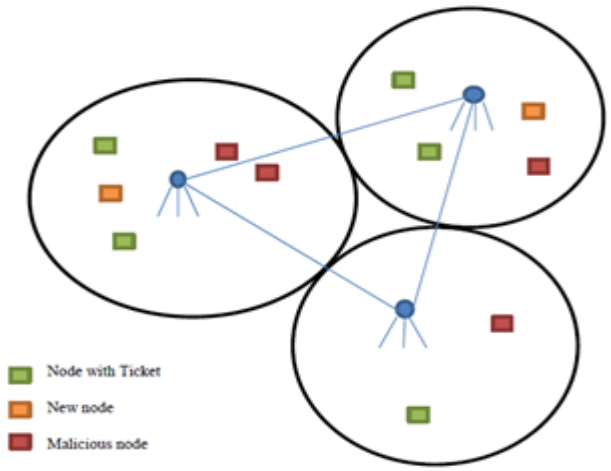

Figure 2: Ticket Granting in MANET

4.2 White List and Black List

Based on the behavior of nodes TGS divide these nodes into well behaved nodes(white list) and malicious nodes(black list). White list nodes are legitimate and further traffic can be passed to them. While selecting a route Black listed nodes are being avoided. So a secure path can be selected by TGS by listing all nodes.

4.3. Tickets

A ticket is a piece of token that allows permission to take part in data communication. Tickets are granted by TGS based on the data forwarding capacity of that particular node. Tickets contain various data fields such as source ID, session key, Time limit, Destination ID etc. Tickets can also include various security parameters. In figure 2 the green colored node is the one which has got the ticket based on its well behavior. Red colored nodes are being black listed and they will not get tickets from any TGS. Orange colored nodes are new nodes that can get ticket on a temporal basis as they may or may not act as malicious.

4.4 TGS-EAACK

Ticket granting is enabled so as to maintain an updated database to store the list of intruders. EAACK doesnot have the method to broadcast the details of intruders in the network. Here a node after receiving a ticket from TGS it sends data by selecting a shortest route. Intrusion detection is being found out according to the working of ACK,SACK and MRA modes. After finding out the intruder it is reported to the TGS and the details are being stored in updated database. A predefined threshold is selected to list a node in blacklist. When a node moves into other range of TGS all the details of the node from previous TGS is to be forwarded to the current TGS. Also an expiry for tickets is set to avoid misusage of tickets.

5. Conclusion

The Ticket Granting based Intrusion detection mainly focuses on security challenges of MANET such as integrity ,non- Secure nodes are being saved and so route selection includes only the secure whitelisted nodes. The scheme works well in mobile and static environments with good packet delivery ratio and throughput. The proposed technique emphasises onrepudiation, authentication and authorization.The scheme mainly focuses to enhance security and to mitigate various network attack issues like partial packet dropping, forged acknowledgments, false misbehaviour reports, receiver collision, and limited transmission. The scheme mainly aims to store the details of all nodes in the network in two lists namely black and white lists according to the successful delivery of packets. EAACK is used to find out the intruders in the network and to report to TGS.Secure nodes are being saved and so route selection includes only the secure whitelisted nodes for further communication.

Licensed Under Creative Commons Attribution CC BY

6. Acknowledgments

Heartfelt thanks to Mr.Sreerag B M and Mr JeswanthSujathan for their valuable contributions in bringing out this novelty for improving the intrusion detection in MANETs.

References

[1] "EAACK—A Secure Intrusion-Detection System for MANETs", Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE
[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Adhoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012.
[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," Proc. 6th Annu.Int. Conf. Mobile Comput.Netw., Boston,
[4] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.
[5] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in Communications in Computer and Information Science,vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384–387.
[6] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, vol. 21, no. 2,pp. 120–126, Feb. 1983.

Licensed Under Creative Commons Attribution CC BY