ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Detecting Forged Acknowledgement in Mobile Ad-Hoc Network Using Intrusion Detection System

Lavanya.K[1]

PG Student, Dept. of CSE, Sri Eshwar College of Engineering, Coimbatore[1]

ABSTRACT: On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

KEYWORDS: ACK, S-ACK, IDS, Security issue, MANET, EAACK.

I. INTRODUCTION

Mobile Ad-hoc network is a self configuring infrastructure which nodes act as a both sender and receiver. In this there is no centralized server for communicating because this network is independent infrastructure[1][2]. Nodes transmit the packets within the range, but it does not transmit the packets when the receiver beyond the limited range. This leads to loss of packets and both the node are reaches within range then it retransmits the packets to respective receiver or node. When the two nodes are sending the packets to another node at the same time then it leads to Packet collision[6]. Then the receiver cannot send the acknowledgement within the time. Then it sends the false acknowledgement to sender and it retransmits the packets.

Here we introduce Intrusion Detection System for detecting the vulnerabilities and malicious attack. Intrusion is used to compromise the security, confidentiality etc., within the nodes and leads to loss of packets and sends the false acknowledgement, negative acknowledgement and vulnerability. The major drawback in this independent infrastructure is the absence of the centralized server for communication. If the nodes transmit the packets bandwidth should be higher but in this network there is only limited bandwidth. This Intrusion Detection System used to detect the malicious attack and the selfish nodes in the MANET. The designing efficient IDS are used to improve the performance of the network. Detecting the intrusion is very difficult in MANET; this can differentiate anomalous activities in network. There different solutions for detecting the malicious attack.

In MANET the packets are sent by the sender and then acknowledgement is received by the sender. When the packets are send to receiver with the intermediate node and it sends the TWO acknowledgements. If the connections are lost then the receiver does not send the acknowledgement, then it doesn't knows what happen to the packets. For this, receiver sends the false acknowledgement then the sender retransmits the packets[8][10]. Another solution for reliability is Flooding-based route discovery in MANETs. This is to set up the route with reliability between sender and receiver. But this approach may cause a serious conflict in information transfer between adjacent nodes and a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

considerable amount of control packets. The transmitting of information between nodes is made secured by Intrusion detection system (IDS)[16]. Not only the packets and also have solution for other security issues in MANET.

MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery[5]. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations.

II. SUSCEPTIBILITY IN MANET

In MANET the vulnerabilities are nature which is harmful to nodes that are transmitting the packets. There is no stable infrastructure leads to lack of boundary and the packets are lost[22]. There are various link attacks that can expose the mobile ad hoc network, which make harder for the nodes in the network to oppose the attacks. These attacks include message relay, eavesdropping, loss of secret data, denial of service.

2.1 IDS Architecture:

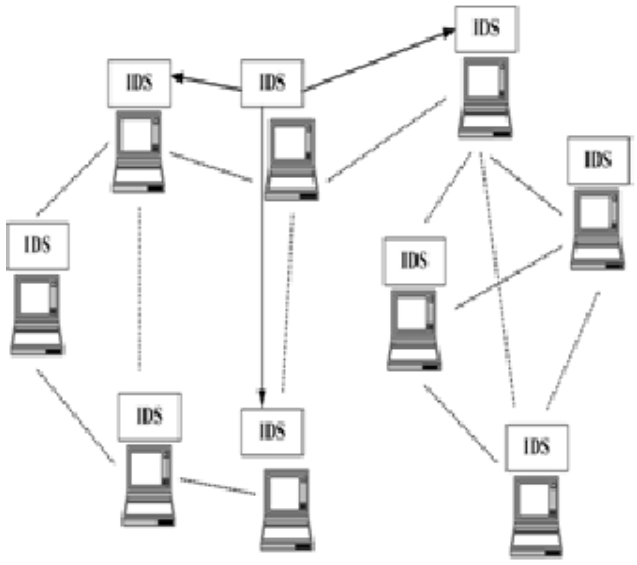

Fig 2.2.1 IDS Architecture

In the IDS architecture there are many numbers of independent nodes which is connected to the Detection system for detecting the malicious attack. Lack of reliability between the nodes leads to inconsistent communication of the nodes. This lacking is due to limited resources for the wireless nodes. Frequent changes in topology due to mobility of nodes and independent infrastructure, this affect the routing information between the nodes[18]. Because of changing topology each node should be incorporate with their neighbor node and to avert from the attacks which may act as liability in the routing protocol. This architecture is used for IDS to detect the vulnerability which separate the anomalous activities in the network.

MANET does not have the centralized system, named server, which leads to some susceptible attacks. In large network it is difficult to identify the traffic and to monitor the system in the network. These attacks are not easy to detect because they often change their pattern within the short time. But this can be found out in system view because

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

these attacks perform various misbehaviors which make system failure. But it can be overcome by considering the trusted nodes. These nodes should be co-operating with network where security is not assumed to all nodes[3][9]. For transmitting the packets to all nodes, cooperative algorithm is used for all nodes and infrastructure. The network is decentralized that breaks the cooperative algorithm and perform the attacks and the vulnerability in networks.

2.2 Limited Power Supply:

In wired network, no need to consider power supply because the power is supplied by the wired one or by their outlets. But in wireless network there is limited power supply to the nodes because of the mobility of the nodes. The nodes are exhausted when it transmit the extra packets which is meaningless one. This may leads to the loss of packets and the power supply is limited which cannot be used for reliable transmission[16][10]. The nodes are behave like a selfish manner to transmit the packets which it doesn't help the other nodes in network. This may because the network vulnerable to the nodes which attacks affects the other nodes in the network. This also uses the clustering scheme to prevent the attacks and the vulnerable of the nodes. Then the monitoring node is assigned for the cluster scheme which is uses the intrusion detection technique which can be considered as the trusted node and no trusted node. These nodes should be trusted for the transmitting the packets and this can prevent from the vulnerable malicious attack.

III. PRECAUTIONS FOR ISSUES

For the above vulnerabilities and the attacks there are much more schemes introduced for the prevention and detection of these attacks. These schemes are used to protect the nodes from the vulnerabilities and from the attacks[17]. This introduces the Intrusion Detection System for the nodes to be prevented from the vulnerabilities.

3.1 IDS Techniques in MANET:

Intrusion is the malicious attack that cannot be detected easily, this can detected by the Intrusion Detection technique. It detects the unwanted attacks nodes and the vulnerabilities. In this technique the IDS Agent is used for the cooperation of the nodes which compromises the security. This agent consists of four modules. These modules ensure that detection of vulnerabilities and the intrusion attacks. In the figure, they represent the four modules which allocating a responsibility to each module. In the first module it checks the data gathered and audit will be done by the different wealth. Next module is to scrutinize the local data and detect any vulnerabilities presence. Third module works with the agent to discover any proof that malicious activities is present. Last module deals with the response that the malevolent attack is confirmed. Using IDS is to prevent the malicious attack and mechanism used is Watchdog, TWOACK, AACK.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

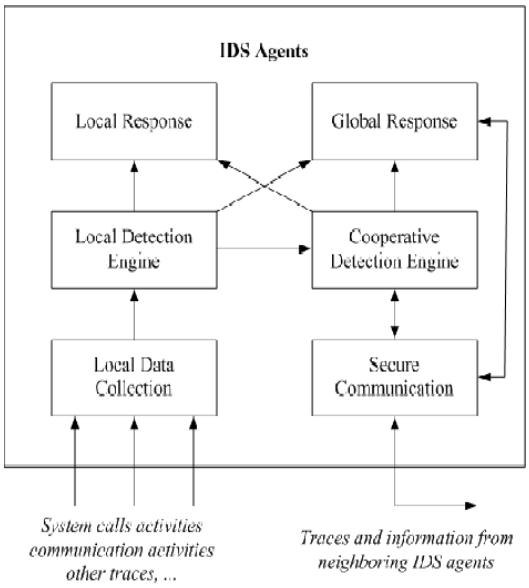

Fig 3.1.1 IDS Agents

3.2 ID Response Technique:

Intrusion response technique is composed of several layers in the detection system for gaining the better performance even though it is affected by the vulnerabilities. The layers considered as the MAC protocol and the application layer[14]. These layer are used in this technique to integrated the attacks are easily find in the higher layer such as application layer than in the lower layer like MAC protocol. Other than the power supply and the selfish manner there is another problem is that overhead. The performance will be lower than the expected one due to the overhead, so multi layer ID technique is used. This IDS agent should be present in layer of each node so that vulnerable can be detected more efficiently.

3.3 Cluster ID Technique:

In the cluster based intrusion detection technique, the nodes which are in network should be cooperative to the other node and network. These may be down due to the battery power and the selfish manner of the node in the network[11]. This technique forms the number of group or cluster in which a node should at least a member of one group. In this there should be a one cluster head to monitor the other nodes and these nodes should be within the radio range[24][21]. Node is selected as head but the other should be within the 1-hop vicinity. The election process is used for the head cluster and this will be select the other nodes to produce better performance and with high efficiency and the probability of the nodes should be equal.

IV. EAACK- SECURE IDS

In MANET, the nodes are connected as the bi-directional link which acts as both sender and receiver. When the node sends the message in the form of packets, it sends back the acknowledgement but cannot find about the forged acknowledgement. For this EAACK approach is used MRA scheme for detecting the forged acknowledgment and report about the packets that send to other nodes. There are more schemes like Watchdog, TWOACK and AACK.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

These schemes have drawbacks like packet collision, loss of packets, false report of packets, limited power, collusion etc. For this a new IDS named EAACK which packets send the report whether it is a false report and the forged acknowledgement.

4.1Watchdog

Watchdog that aims to improve the throughput of network withthe presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network[19]. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving[20]. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.
Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field[23]. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

4.2 TWO ACK

This secure IDS is used to detect the false misbehavior by the TWO ACK. The solutions for secure IDS given by S-ACK, MRA (Misbehavior Report Authentication) and ACK.

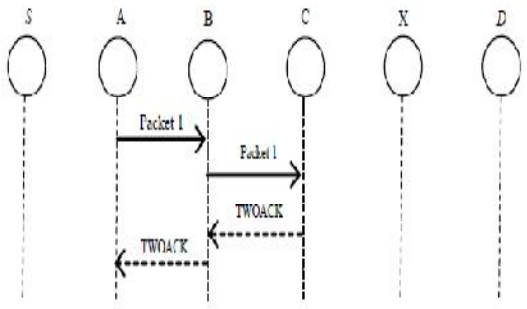

Fig 4.2.1 TWOACK

In this TWOACK, there are 3 nodes which node A sends the packet to node C which is an intermediate node B. When A sends the packet to B which in turn sends to node C and it responds with the acknowledgement from C to B then from B to A. when the acknowledgement is not received then the sender believes that packet is loss due to network connection and it retransmits the packet to intermediate node.

4.3 AACK

AACK(Adaptive ACKnowledgement) is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. The end-to-end acknowledgment scheme in ACK is shown in Fig. 4.3.1 In the ACK scheme shown in Fig. 4.3.1, the source node S sends out Packet 1 without

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

any overhead except 2 b of flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful.

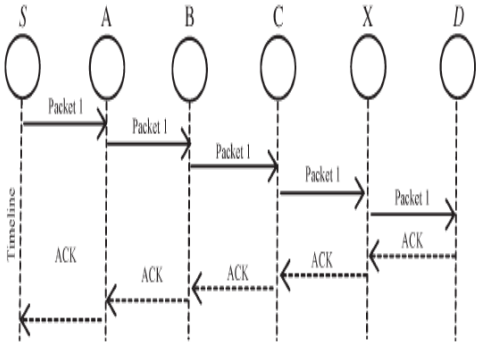

Fig 4.3.1 AACK Scheme

Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehaviour report and forged acknowledgment packets. In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic.

V. CONCLUSION AND FUTURE ENHANCEMENT

In this paper we discuss about the security issues in MANET and it can be prevent using the Intrusion Detection System. Using IDS there are many solution are given but there are drawbacks in reply with the acknowledgement that gives report. But this report never specifies the details of packets whether it is losses the packet or collision, or due to mobility of the nodes. Our future enhancement is said to overcome the report of the packets and say about the packet and their details. These have their IDS named EAACK used to detect the forged acknowledgements using the Digital Signature Algorithm (DSA) and compare with the RSA algorithm through Simulation.

REFERENCES

[1] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.
[2] M. Weiser, the Computer for the Twenty-First Century, Scientific American, September 1991.
[3] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.
[4] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.
[5] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.
[6] Y. Hu, A. Perrig and D. Johnson, Wormhole Attacks in Wireless Networks, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.
[7] A. Perrig, R. Canetti, J. D. Tygar and D. Song, Efficient Authentication and Signature of Multicast Streams over Lossy Channels, In Proceedings of the IEEE Symposium on Research in Security and Privacy, pages 56–73, May 2000.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[8] Jim Parker, Discussion Record for the 1st MANET Reading Group Meeting, http://logos.cs.umbc.edu/wiki/eb/index.php/February_10%2C_2006 (Authorization required).
[9] Architecture for reliable server pooling [Online]. Available: www.ietf.org/ids.by.wg/rserpool.html
[10] M. Fecko, U. Kozat, S. Samtani, M. Uyar, and I. Hökelek, "Architecture and applications of dynamic survivable resource pooling in battlefield networks," in Proc. SPIE, vol. 5441, Bellingham, WA, 2004, pp.
204–214.
[11] U. C. Kozat and L. Tassiulas, "Service discovery in mobile ad hoc networks: An overall perspective on architectural choices and network layer support issues," Ad Hoc Netw., vol. 2, no. 1, pp. 23–44, Jan. 2004.
[12] G. Di Crescenzo, G. R. Arce, and R. Ge, "Threshold cryptography for mobile ad hoc networks," in Lecture Notes in Computer Science. NewYork: Springer-Verlag, 2004, vol. 3352, Proc. Security in Commun., pp. 91–104.
[13] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Commun., vol. 11, no. 1, pp. 38–47, Feb. 2004.
[14] Y.-C. Hu and A. Perrig, "A survey of secure wireless ad hoc routing," IEEE Security and Privacy, pp. 28–39, May/Jun. 2004.
[15] B. C. Neuman and T. Ts'o, "Kerberos: An authentication service for computer networks," IEEE Commun. Mag., vol. 32, no. 9, pp. 33–38, Sep. 1994.
[16] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. ACM Comput. Commun. Security, Washington, DC, Nov. 2002, pp. 41–47.
[17] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.
[18] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," ACM Trans. Program. Languages Syst., vol. 4, no. 3, pp. 382–401, Jul. 1982.
[19] A. Boldyreva, "Efficient threshold signatures, multisignature and blind signature schemes based on the Gap–Diffie–Hellman-group signature scheme," in Lecture Notes in Computer Science. News York: Springer- Verlag, 2003, vol. 2567, Proc. Public-Key Cryptography, pp. 31–46.
[20] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil Pairing," in Lecture Notes in Computer Science. News York: Springer-Verlag, 2001, vol. 2248, Proc. Advances in Cryptology—Asiacrypt, pp. 514–532.
[21] J. Katz and M. Yung, "Threshold cryptosystems based on factoring," in Lecture Notes in Computer Science. News York: Springer-Verlag, 2002, vol. 2501, Proc. Advances in Cryptology—Asiacrypt, pp.
192–205.
[22] T. Pedersen, "A threshold cryptosystem without a trusted party," in Lecture Notes in Computer Science. News York: Springer-Verlag, 1991, vol. 547, Proc. Advances in Cryptology—Eurocrypt, pp. 522–526.
[23] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," Proc. ACM MobiCom '00, Aug. 2000.
[24] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive Secret Sharing or: How to Cope with Perpetual Leakage," Proc. CRYPTO '95, pp. 339-352, 1995.