International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 04, April 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

INTRUSION DETECTION SYSTEM USING EAACK ALGORITHM

Anu B[1], Devi R[2], Laya K Roy[3], Meha S N[4]

[1, 2, 3, 4]*Computer Science and Engineering, Nehru College of Engineering and Research Centre,(India)*

ABSTRACT

Wireless Mobile ad-hoc network (MANET) is an emerging technology. MANET is infrastructure less, without centralized control. Each node acts as router. Each device in a MANET is independently freely moves in any direction. In MANET, each node in a network performs as both a transmitter and a receiver. MANET is vulnerable to passive and active attacks due to its open medium, changing topology and lack of centralized control. Many existing IDSs for MANETs are based upon Watchdog, TACK and AACK mechanisms. Nodes in MANETs communicate with each other via bidirectional wireless links either directly or indirectly. A new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs to overcome DDoS attack is proposed in this paper. EAACK demonstrates higher malicious-behavior-detection and prevention rates.

Keywords- Security, Mobile Ad-hoc Network (MANETs), Enhanced Adaptive Acknowledgment (EAACK), Algorithms, Distributed denial of service attack.

I. INTRODUCTION

A mobile ad hoc network (MANET) is an infrastructure-less network of mobile devices connected without wires. Its self-configuring nature makes it popular among networks. Each device in a MANET is free to move independently in any direction. Each will act as a receiver and transmitter and each sends traffic unrelated to its own use, and therefore be a router. MANET allows data communication with different parties maintaining mobility of devices. A node can join or leave the network independently. Two nodes in MANET cannot communicate if they are beyond a certain range. This problem is solved by allowing intermediate between sender and receiver nodes. MANETs are mainly divided in to two as single hop and multi hop. MANET is a self-configuring and self-maintaining network. It functions without a centralized architecture. The major attack in a ad-hoc network is DDoS [1] attack, Where the genuine user does not get the service from a server due to unauthorized access. One of the primary issues related to ad hoc network is to provide a secure communication among mobile nodes. MANETs consist of a peer-to-peer; self-forming, self-healing network without a centralized control.

II. EXISTING SYSTEM

There exists several IDS system to prevent DDoS attacks in MANETs. There exist mainly three systems such as Watchdog, Two ACK and AACK.

- Watchdog: Watchdog aims to improve the throughput of network with the presence of malicious nodes. Scheme is consisted of two parts, Watchdog and Path rater. Watchdog is responsible for detecting malicious nodes in the network. If a Watchdog node overhears that a node is misbehaving or fails to forward a data packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined value, the Watchdog node reports it as misbehaving. The Path rater avoids the reported nodes in future transmission. The Watchdog Scheme fails to detect: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehaviour report; 5) collusion; and 6) partial dropping [2].
- ACK: Each node sends back an acknowledgment packet to the node that is two hops away from it. This same process applies to every three adjacent nodes along the rest of the route. The acknowledgment process required in every packet transmission process causes unwanted network overhead, which is considered as a disadvantage of TACK scheme. It resolves the receiver collision and limited transmission power problems of Watchdog [3].
- AACK*:* Based on TWOACK, a new scheme called AACK. Similar to TWOACK, AACK 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[4].

III. PROPOSED SYSTEM

The main security attack in Mobile Adhoc Network is DDoS attack and there exists several Intrusion Detection Systems to prevent such security threats. These existing IDS systems in wireless sensor network use two main intrusion detection parameters namely Packet Reception Rate (PRR) and Inter Arrival Time (IAT). But these parameters are not good enough to detect the security attacks. So the proposed IDS system adds other parameters into it and makes it works more accurately. The proposed system uses Enhanced Adaptive Acknowledgment (EAACK) and Adhoc On demand Distance Vector (AODV) protocol. EAACK algorithm is designed to tackle three of the six weaknesses of old IDS systems namely false misbehavior, limited transmission power, and receiver collision [5].

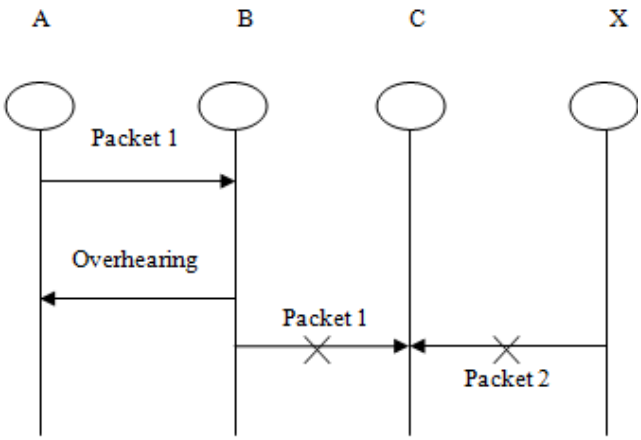

Fig.1. Receiver Collision

Fig.1. represent the receiver collision problem. Node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C, at the same time node X is forwarding Packet 2 to node C. In such case, node A overhears that node B has successfully forwarded Packet 1 to node C but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

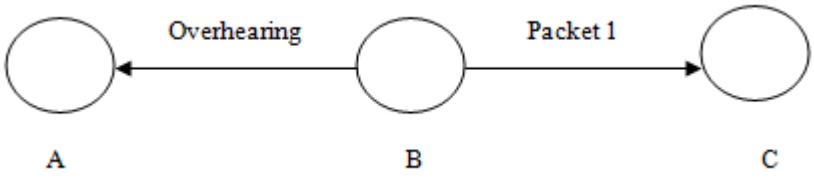

Fig.2. Limited Transmission Power

Limited transmission power is represented in Fig.2. In the case of limited transmission power, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C

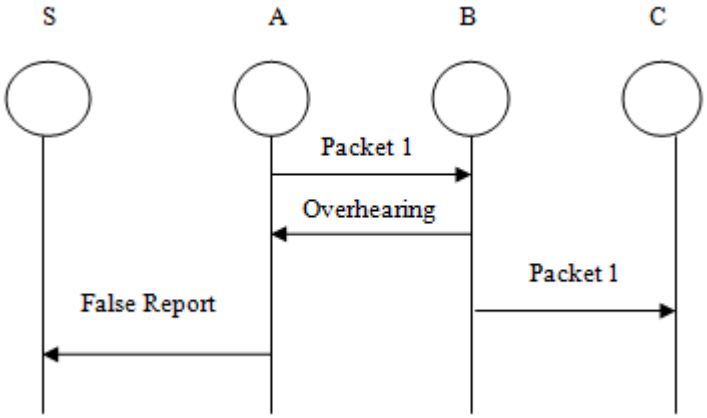

Fig.3. False Misbehavior

False misbehavior is represented in fig.3. Node A successfully overheard that node B forwarded Packet1 to node C, node A still reported node B as misbehaving. Open medium and remote distribution are two important features of Mobile Adhoc Network. Due to these two features of MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack. The existing IDS systems such as TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehavior attack. In this research work, this system proposes new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem.

The proposed system deals with EAACK algorithm with AOD protocol. EAACK algorithm generally consist of three major parts namely ACK, SACK and MRA. The system uses the concept of digital signature for providing better encryption and security for data.

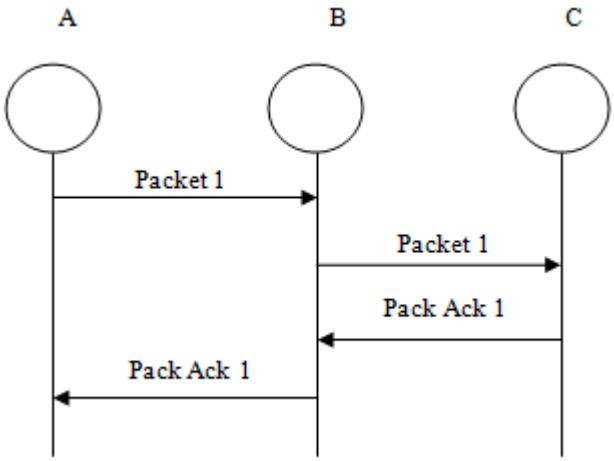

Fig.4. ACK Scheme

Fig.4 represents the ACK scheme. Here node A is sending data packets to node B. When the packets arrived in node B, the node generates ack packets and resends it to node A.

- ACK

The first major component of EAACK algorithm ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK. Important aim is to reduce network overhead when no network misbehavior is detected. Similarly node B is forwarding the packets to node C and C resend ack packets to node B [6].

- S-ACK

The second major component of EAACK, The Secured ACK (S-ACK) scheme is an improved version of the TWOACK scheme. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power [7].

- MRA

Third major components of EAACK algorithm is Misbehavior Report Authentication (MRA). The MRA scheme is designed to resolve the weakness of existing IDS Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report is generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The main idea of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes, by adopting an alternative route to the destination node [8].

- DIGITAL SIGNATURE

Digital signatures are standard element of cryptographic protocol. They are used to demonstrate the authenticity of digital message or document. Valid Digital signature scheme gives a reason to believe that the message was

created by a known sender and that the message was not altered. So this scheme of cryptography deals about authentication, non repudiation and integrity. They are the public key primitives of message authentication. Digital signature concept is used to bind signatory to the message and it also binds a person or entity to the digital data. This is a cryptographic value calculated from the data and a secret key known only by the signer. The proposed system uses the concept of digital signature to provide more security to the data. The system encrypts the message at sender side using the concept of digital signature and also decrypting the message at receiver side [9].

IV. IMPLEMENTATION

The proposed system can be implemented using java with jdk version 1.6 as front end and My SQL as back end. The database is connected with the front end using JDBC.

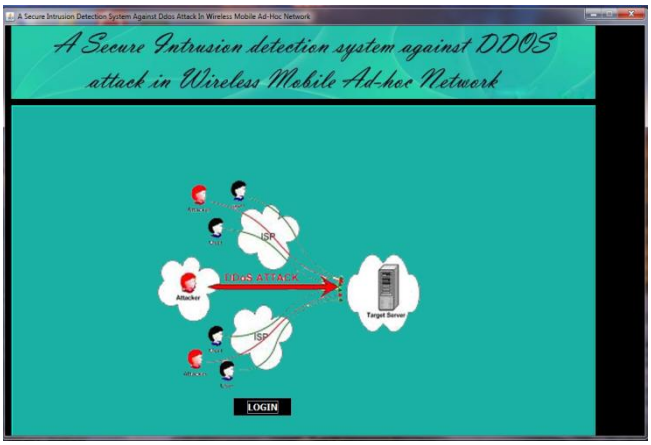

Fig.5. Home Page

Fig.5. indicate the home page of the system. A new user can login to the system with the help of this page.

The procedure of the system can be represented by using a data flow diagram. Data flow diagram shows relationships among and between the various components in system.DFD is simple graphical formalism and also known as

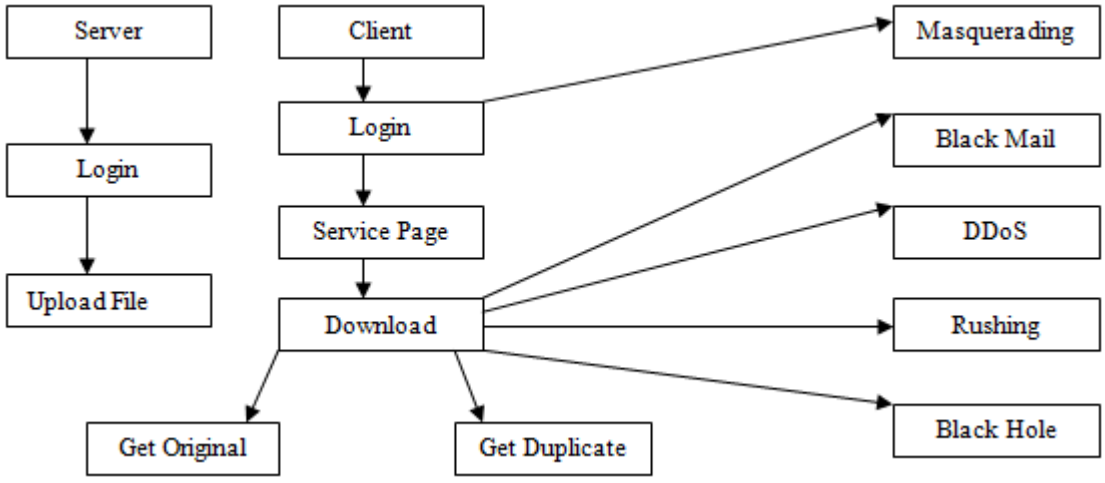

Fig.6. Data Flow Diagram

Fig.6. illustrates Data flow diagram. Here, communication between client and server occurs. Server logins to the system with their own username and password. Server uploads file to the system. Client downloads the file by logging in with their own IP Address and password. The uploaded file is encoded at the server side and decoded at client side. The entire data will divided into seven segments and encoded to ASCII digits. The client receives acknowledgment for each of the data packets received. The authenticated client can download the required file from the system.

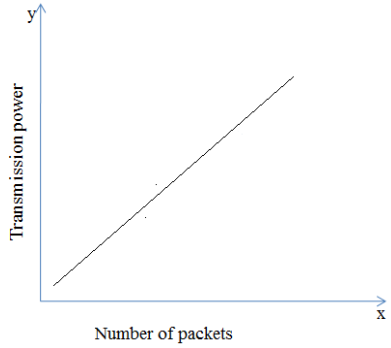

Fig.7. Graphical relationship between transmission power and number of packets

Fig.7. shows graphical relationship between transmission power and number of packets. If increases no of packets that are send by the server due to increase the overall transmission power. The transmission power is directly propositional to the number of packets.

The following attacks are detected by the IDS system using EAACK [2] algorithm. The IDS system using EAACK algorithm is detecting the presence of several attacks and are [10],

- Masquerade Attack: A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network.
- Black mail Attack: Blackmail or extortion often involves a threat to spread information about the target that will defame his or her reputation or bring criminal actions against him or her unless some amount of money is paid to the individual making the threats. In the network some time intruder ask password of the user when he download particular file from the system. If the client enters correct or incorrect values, so that intruder can trap the personal details.
- DDoS Attack: DDoS attack is a major problem in MANET and in all Adhoc networks. DDOS is where the attack source is more than one, often thousands of, unique IP/network addresses. DDOS attack occurs when more than one system floods the bandwidth or resources of a targeted system, usually one or more web servers and network traffic is created. A botnet is a network of zombie computers programmed to receive commands without the owners' knowledge. The main advantage of DDoS attack is multiple system can generate more traffic attack than the one system.
- Rushing Attack: An offensive that can be carried out against on-demand routing protocols is the rushing attack on-demand routing protocols state that nodes must forward only the first received Route Request

from each route discovery; all further received Route requests are ignored. This is done in order to reduce cluttering. The attack consists, for the adversary, in quickly forwarding its Route Request messages when a route discovery is initiated. If the Route Requests that first reach the target's neighbors are those of the attacker, then any discovered route includes the attacker.

- Black Hole Attack: Black hole refer to places in the network where incoming or outgoing traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient. In this attack that changes entire file contents to some other form. Client receives unwanted or duplicated data. A black hole e-mail address is an e-mail address which is valid (messages sent to it will not generate errors), but to which all messages sent are automatically deleted, and never stored or seen by humans. These addresses are often used as return addresses for automated e-mails

V. CONCLUSION AND FUTURESCOPE

One of the major threats to the security in MANETs is the packet dropping attack. This research paper proposes a specially designed protocol for MANETs, that is a novel IDS named EAACK. Some of the limitations of Watchdog, TWOACK and AACK such as receiver collision, limited transmission power and false misbehavior are effectively overcome by proposed EAACK approach. It also eliminates the need for a centralized trusted authority which is not practical in ad-hoc network due to their self-organizing nature. The proposed mechanism demonstrates that the presence of DD0S increases the packet loss in the network. The EAACK approach protects the network through a self-organized fully distributed and localized procedure. Another advantage of this mechanism is that it can be applied for securing the network from other routing attacks. This is achieved by changing the security parameters in accordance with the nature of attack. In order to prevent the forged acknowledgement attacks digital signature can be incorporated in the proposed scheme. This will improve the network's PDR when the attackers are smart enough to forge acknowledgement packets. However it will generate more routing overheads in some cases. Thus this tradeoff is worthwhile when network security is the top priority.

REFERENCES

[1] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[2] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.

[3] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in Proc. 3rd Int. Conf. Pervasive Comput. Commun., 2005, pp. 191–199.

[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer- Verlag, 2008.

[5] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[6] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow,Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[7] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf. Perform., Comput.,Commun., 2004, pp. 747–752.

[8] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput.,vol. 6, no. 5, pp. 536–550, May 2007.

[9] 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.

[10] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf., 2003, pp. 75–78.