ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Insider Attack Detection System (IADS) in MANETs

Rangachary K[1], Dr.S.Naganjaneyulu[2]

PG Scholar, Software Engineering, LBRCE, Mylavaram, India

Professor, Information Technology, LBRCE, Mylavaram, India

Abstract: The migrating towards wireless network from wired network has become latest popular global trend in past few decades. The versatile properties of wireless networks created it possible in countless applications. Involving all of the contemporary wireless networks, Mobile Adhoc NETwork (MANET) provides essential and unique applications. Because of its awesome abilities like mobility, scalability and self configuration, the MANET has been wide spread in many applications like military, rescue operations, some tactical conditions and the like. The intrinsic nature of Adhoc networks makes them vulnerable to various passive and active attacks and thus it is vital to build an efficient intrusion detection mechanism to protect MANET from attacks. Prevention methods for attacks alone are not sufficient to make them secure. So, Intruders have to be detected at the early stages of data transmission. To acquire security we are proposing A Novel Intrusion detection system (NIDS) named Enhanced Adaptive ACKnowledgement (EAACK) is introduced for Insider Attackers (IA) in MANETs by using normal end to end ACK scheme, Secure ACK (S-ACK) and Misbehavior report Authentication (MRA) scheme. The proposed system eliminates the existing system weaknesses like Receiver Collision, Limited Transmission power and false misbehavior report. EAACK yields better results compared to all modern techniques for misbehavior detection by reducing the routing overhead and by increasing the network performance. The three parts of EAACK (ACK, SACK and MRA) are acknowledgement based detection systems. To detect the misbehaviors in the network, the three schemes rely on ack packets. All ack packets are authentic and untainted. Otherwise the attackers forge the ack packets. So, we include Digital Signature in EAACK to ensure the integrity of Intrusion Detection system.

Keywords: MANET, Insider attack, Digital Signature Algorithm (DSA), MRA.

I. Introduction

In Latin Adhoc means “for this”, further meaning “for this purpose only”.Adhoc nodes are temporary network, setup anywhere without any need of external infrastructure like wires or base stations [5] [10] [20]. By definition, Mobile Adhoc NETwork (MANET) is a collection of mobile nodes equipped with both transmitter and receiver that communicate with each other via bidirectional wireless links directly or indirectly [6]. The best examples of MANET nodes are mobiles, laptops, PDAs etc. These nodes are vulnerable to attacks due to the following reasons: [9]

- Because of limited transmission power complex security mechanisms cannot be applied.
- Data transmission is done by wireless medium.
- Due to decentralized nature it is difficult to ensure whether all nodes are participating in data transmission compassionately.
- Fixed routing is not available.

Even though MANETs are suffering with these issues, there are several reasons for their popularity .Those are:

- Dynamic network configuration.
- Low cost of deployment.
- Easy to use.

Due to the limited range of nodes, two nodes cannot communicate each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by introducing intermediate nodes. To achieve this MANET is divided into two types. Single hop and Multi hop. In a single hop network, all nodes in same radio range can communicate directly. In multi- hop network, nodes rely on their intermediate nodes for data transmission.

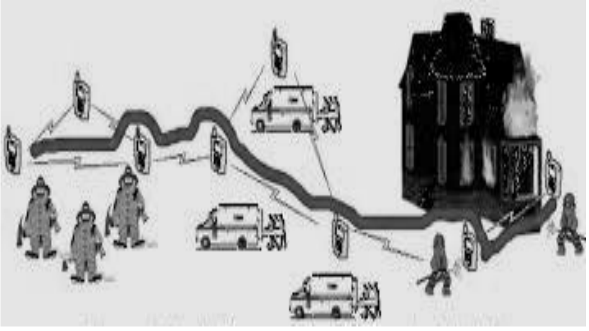


Fig. 1 Multi Hop Communication in MANETS

II. Background

A. Intrusion detection System

Intrusion Detection can be defined as the technique to identify “any set of actions that attempt to compromise the security attributes like availability, integrity, confidentiality of any resource”. The mechanism which performs this task is called Intrusion Detection System [2] [3]. In MANETs the general functionality of IDS is to identify the intruders/attackers who are misbehaving in the network. The attacks in MANET can be classified according to its domain, protocols and the way how the attack can effect.

DOI 10.17148/IJARCCE.2015.4662

According to the third type, the attacks are of two types:

Active and passive attacks. Passive attacks are those in which the intruder obtains data but not disrupting it, while an active attack involves interrupting the information, modification, thereby disturbing the normal functionality of data transmission. According to domain of the attacks, the attacks can be classified into two categories: Insider and Outsider attacks.

Insider attacks are done by compromised nodes, which are actually the part of MANET network. Outsider attacks are carried out by outside or external nodes. Outsider attacks are easy to recognize and can be detected/prevented with cryptographic techniques (Encryption, Decryption, Private Key) [11] [12] [13]. However, insider attacks are very complicated. These attacks cannot be prevented with simple cryptographic techniques.

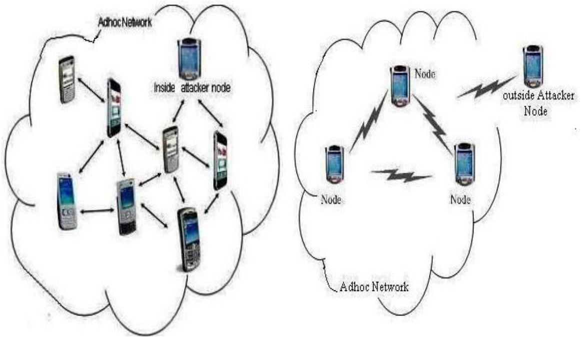


Fig.2 Insider and Outsider Attacks in MANETs

Various Intrusion detection Systems (IDS) are proposed to detect the attackers. Some IDS methodologies are:

A. Anomaly based

The first technique considers the behavior of the system like frequently used commands, CPU usage for programs, and the like. This technique notices intrusions as anomalies.

Various techniques are proposed for this. i.e., Statistical approaches and artificial intelligence etc. Normal behaviors may change over the time. The IDS mechanism must be kept up to date. This is the fine technique for the nodes which are existed for a long period of time. If any node is newly joined in the network and is participated in any malicious action then the anomaly detection is futile.

B.Misuse-based

This mechanism compares known attack signatures with current system activities. It is generally used by commercial IDs which yields low false reports. The drawback of this technique is it cannot detect new attacks like anomaly based technique.

C.Specification-based

In this approach, a set of constraints on a program or a protocol are specified and intrusions are detected as runtime violations of these specifications. This technique combines the strengths of Anomaly and misuse based techniques. It can detect the misbehavior which does not follow the specifications. It has been applied to ARP (Address Resolution Protocol) and DHCP (Dynamic Host Configuration Protocol) and many routing protocols.

The three main components of IDS:

- Collection Phase (Collecting the data)
- Detection Phase (Analyzing the data)
- Response phase (Respond by alert when intruders are detected).

B. IDS in MANETs

IDS s usually acts as second layer in MANETs and they are a great complement to existing proactive approaches [4]. Anantvalle and Wu [14] presented very tough survey on contemporary IDSs in MANETs. In this section we mainly describe three existing techniques namely,

1)Watchdog
2)TWOACK and
3)Adaptive ACKnowledgement (AACK)

1. Watchdog:

Marti et al. [17] proposed a scheme named Watchdog that aims to improve throughput of network in the presence of malicious nodes. In fact, the Watchdog scheme consisted two parts, namely, Watchdog and Pathrater. Watchdog serves as IDS for MANETs. It is responsible for detecting malicious misbehaviors by promiscuously listening to its next hop's transmission. If the Watchdog node overhears that its next node is fails to forward the data within a certain period of time, it increases the failure counter. Whenever a node's failure counter exceeds predefined threshold, the watchdog node reports it as misbehavior. In this case, Pathrater cooperates with the routing protocols to avoid the reported node. Many research applications and MANET IDSs are developed based on this technique. Even though it provides handful of benefits, it is suffered with several weaknesses. Those are: 1) Ambiguous collisions 2) Receiver collisions 3) Limited Transmission Power 4) False misbehavior report 5) Collusion and 6) Partial dropping [8] [9] [15].

2. TWOACK:

With respect to the six weaknesses of the watchdog, numerous researchers proposed new approaches to crack these issues. Out of those TWOACK is most popular approach proposed by Liu et al. [16].TWOACK is neither enhancement nor a Watchdog based scheme. The main aim of this is to resolve the receiver collision and limited transmission power problems of Watchdog scheme. TWOACK determines the misbehavior by acknowledging every data packet transmitted over every three consecutive nodes along from source to destination. After receiving the packet, each node has to send acknowledgement back to the node that is two hops away from it down the route. The below figure depicts the concept of this mechanism.

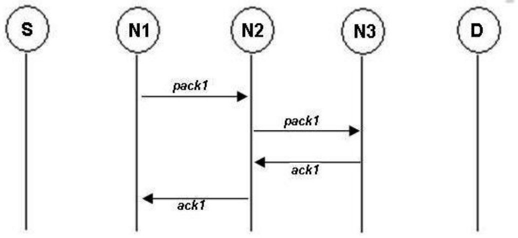


Fig. 3: TWOACK Scheme

DOI 10.17148/IJARCCE.2015.4662

1. AACK:

Based on TWOACK, Sheltami et al. [19] proposed a new scheme, namely AACK which is the combination of TACK (identical to TWOACK) and end to end acknowledgement (ACK). Compared to TWOACK, AACK significantly reduces the network overhead by maintaining the same network throughput.

In ACK, the source sends data packet to destination via intermediate nodes. After receiving the packet the destination acknowledges in reverse order. Within predefined time period, if the source receives the ack packet then the packet transmission from source to destination is successful. Otherwise the source will switch to TACK mode by sending out a TACK packet. It reduces the network overhead. But both TACK and TWOACK still suffer from false misbehavior report problem. i.e., the malicious node may send false report to the source. Hence it is crucial to authenticate the ack packet. To address this problem Enhanced AACK (EAACK) mechanism is introduced, which uses the concept of Digital Signature.

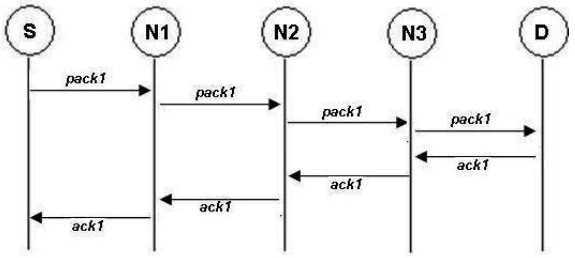
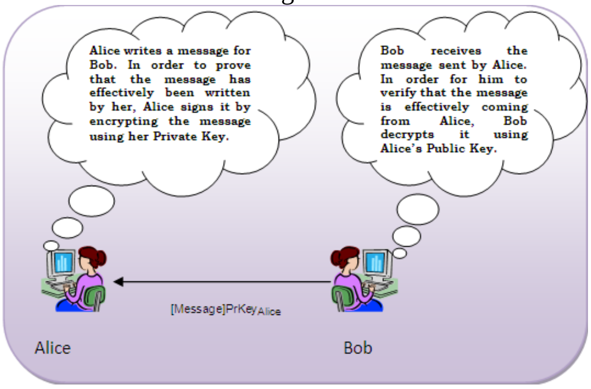


Fig. 4: AACK Scheme

2. Digital Signature

A Digital Signature is a mathematical scheme for demonstrating the authenticity of a digital message or document [18]. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity).It is a mechanism where a message is authenticated.


Alice writes a message for Bob. In order to prove that the message has effectively been written by her, Alice signs it by encrypting the message using her Private Key.

Bob receives the message sent by Alice. In order for him to verify that the message is effectively coming from Alice, Bob decrypts it using Alice's Public Key.

Fig. 5: Digital Signature /verification principles

III. Scheme Description

In this section we describe our proposed scheme EAACK in detail [1]. EAACK consists of three parts, namely, ACK, SACK (Secure ACKnowledgement) and MRA (Misbehaviour Report Authentication). In our proposed scheme, we assume that the link between each node is bidirectional and. source and destination nodes are authentic.

A. *ACK:*

As discussed above ACK is basically end to end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce the network overhead when no network misbehavior is detected. As represented in fig 4, in ACK mode, node *S* first sends out an ACK data packet p*ack1* to the destination node *D*. If all the intermediate nodes in the path are cooperate then node *D* successfully receives the packet p*ack1*.Now the destination *D* has to send back an ACK packet *ack1* to the *S* along the same path, within a predefined time. If *S* receives the *ack1* then the packet transmission is successful and there is no intruder existed in the network. Otherwise *S* switches to S-ACK mode by sending ACK data packet.

TABLE I: Packet type Indicators

Packet type	Packet Flag
General data	00
ACK	01
S-ACK	10
MRA	11

B. *Secure ACK:*

The S-ACK scheme is improved version of TWOACK scheme proposed by Liu *et al.* [16]. In this technique every three successive nodes work as a group to detect the misbehaviours. For every three consecutive nodes in the network, the third node is required to send secure acknowledgement packet to the first node. The main aim to introduce this technique is to detect misbehaviours in the presence of receiver collision and limited transmission power. As shown in fig 6, the three nodes (*N1, N2, and N3*) work as a group.

Node *N1* first sends out S-ACK data packet p*sd1* to the node *N2*.Then, node *N2* forwards this packet to node *N3*.After receiving the packet *N3* acknowledges p*sack1* to *N2*, which again forward it to *N1*. If *N1* doesn't received ack within a specified time period both *N2* and *N3* are reported as malicious and a malicious report is generated by *N1* and will be forwarded to *S*.

However, unlike TWOACK mode, where the source immediately believes the misbehaviour report, EAACK checks the report with MRA mode.

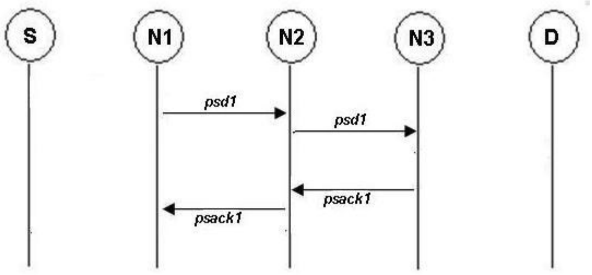


Fig. 6: S-ACK Scheme

C. *MRA (Misbehaviour Report Authentication):*

The MRA scheme is designed to resolve the weakness of Watchdog which was failed to detect the misbehaviours in the presence of false misbehaviour report. The malicious nodes may present the false report as "candid nodes as nasty" or "nasty nodes as candid". To initiate MRA mode, the source first searches its local knowledge base and seeks for alternative route to the destination node. If the search returns null, source bring into play DSR (dynamic Source Routing) to find another route. Due to the nature of MANETs, it is easy to find several routes for data transmission. After getting the path, the source sends same data packet to the destination via second path. After receiving the ack packet from destination the source node checks whether the ack packet is already existed in its knowledge base or not. If not exists, the report is accepted and valid. Otherwise the report is considered as FMR (False Misbehaviour report) and who generated this report will be treated as Intruder. By adopting MRA mode, EAACK is proficient of detecting misbehaviours despite the existence of FMR. The below figure explains MRA scheme. (Where S->N1->N4->N5->D is the alternative path)

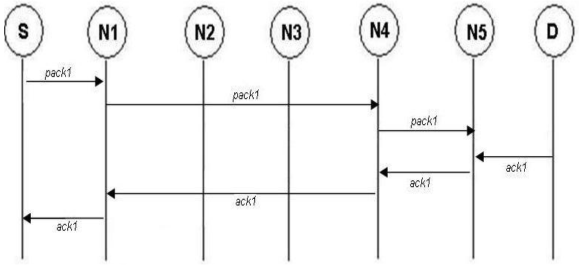


Fig. 7: MRA Scheme

D. *Digital Signature:*

Digital signatures play a vital role in cryptography. It mainly comprises of three Algorithms; [7]

- A *key generation algorithm* that selects randomly a private key uniformly among possible private keys. This algorithm results a set which consists a private key and corresponding public key.
- A *signing algorithm* that results a signature by using private key and message.
- A *signature verifying algorithm* authenticates the message by using public key of the sender and received message.
- The below diagram depicts the procedure followed by the digital signature.

Global Public Key Components

p prime number where $2^{L-1} < p < 2^{L}$ for $512 \le L \le 1024$ and L a multiple of 64 i.e., bit length of between 512 and 1024 bits in increments of 64 bits.

q prime devisor of (p-1),where $2^{159} < q < 2^{160}$ i.e., bit length of 160 bits.

g $= h^{(p-1)/q} \bmod p$ where h is any integer with 1<h<(p-1)such that $h^{(p-1)/q} \bmod p > 1$

User's Private Key

x random or pseudonym integer with 0<x<q

User's Public Key

y $= g^{x} \bmod p$

User's Per-message secret Number

k =random or pseudonym integer with

Signing

r $=(g^{x} \bmod p) \bmod q$
s $[k^{-1}(H(M)+xr)] \bmod q$
Signature=(r,s)

Verifying

W $=(s^{-1})^{-1} \bmod q$
u1 = [H(M')w]mod q
u2 = (r')w]mod q
v $=[(g^{u1}y^{u2}) \bmod p] \bmod q$
TEST: v=r'

M=message to be signed
H (M) = Hash of Musing
SHA-1
M', r', s'=received versions of
M, r, s

Fig. 8: Digital Signature Procedure

IV. Conclusion and Future Enhancement

To provide security in the MANET we introduced Insider Attack Detection System (IADS) called EAACK .By adopting Digital Signature into our proposed scheme we can eliminate the problem of forged acknowledgement. In the EAACK the ack packets are digitally signed by which we can provide authentication for the packets.

To increase the security we plan to investigate the following issues into our future research work.

a) Adopting Hybrid Cryptography techniques to reduce the network overhead caused by Digital signatures.
b) Adopting Key distribution protocols by eliminating pre distribution of keys.
c) Instead of software simulation test the performance of proposed system in real time environment.

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] Investigating Intrusion and Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes Marjan Kuchaki Rafsan,Ali Movaghar and Faroukh Koroupi,World Academic of Science Engineering and Technology 44 2008.

[3] L. Zhou, Z.J. Haas, Cornell Univ., "Securing ad hoc networks," IEEE Network, Nov/Dec 1999.

[4] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[5] G. Jayakumar and G. Gopinath, "*Ad hoc* mobile wireless networks routing protocol—A review," *J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582.2007.

[6] 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.

[7] http://en.wikipedia.org/wiki/Digital_signature.

[8] Investigating Intrusion and Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes Marjan Kuchaki Rafsan,Ali Movaghar and Faroukh Koroupi,World Academic of Science Engineering and Technology 44 2008.

[9] L. Zhou, Z.J. Haas, Cornell Univ., "Securing ad hoc networks," IEEE Network, Nov/Dec 1999,B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation.

[10] Texas A&M Univ., College Station, TX, 2004.A.Janani, A.Sivasubramanyam "Survey of Packet Dropping Attack in MANET", in IJCSE Vol5 No: 1 Feb-Mar 2014.

[11] 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.

DOI 10.17148/IJARCCE.2015.4662

[12] 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.

[13] L. Zhou and Z. Haas, "Securing ad-hoc networks," IEEE Netw., vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

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

[15] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[16] 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.

[17] 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.

[18] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996, T-37.

[19] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs,"*Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[20] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 840–849, Mar. 2010.

BIOGRAPHIES

Rangachary K is a PG Scholar in Software Engineering, Lakireddy Bali Reddy College of Engineering, and Mylavaram.

Dr.S.Naganjaneyulu.,M.Tech.(CSE),PhD Working as Professor in Department of IT, Lakireddy Bali Reddy College of Engineering, Mylavaram from June'2014 to till date. He is Brainbench Certified Professional in Visual Basic 6.0, Java 2, Java EJB, ASP, and C++.

DOI 10.17148/IJARCCE.2015.4662