International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

New Approach of Intrusion Detection for Malicious Behavior Detection in MANETS

Aruna P Adhav, K T Jadhao

[1]Department of Electronics and Telecommunication, Alamuri Ratnamala Institute of Engineering and technology, A.S.Rao Nagar, Sapgaon, Shahapur, Thane, Maharashtra 400708

[2]Professor, Department of Electronics and Telecommunication, Alamuri Ratnamala Institute of Engineering and technology, A.S.Rao Nagar, Sapgaon, Shahapur, Thane, Maharashtra 400708

Abstract: ***Mobile Ad hoc Networks (MANET) lacks fixed infrastructure in which nodes communicate directly with each other when they are both within the same communication range. 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. Due to lack of central control, an intermediate node may drop the data packets because of being selfish or malicious. In this case, it is crucial to develop efficient intrusion-detection system (IDS) to protect MANET from attacks. One of the IDS called Watchdog scheme failed to detect malicious misbehaviors with the presence of various misbehavior activities from which some of them can be removed by various acknowledgment based methods but these methods failed to remove all the attacks. An IDS named Enhanced Adaptive ACKnowledgment (EAACK) with digital signature designed for MANETs try to detect malicious node in some cases but still failed to give complete result. Here we propose the design of a simple yet effective NACK in which the new ACKnowledgement-based scheme, called NACK and Combination of DSA and RSA cryptography is introduced in EAACK based on the DSR protocol. As per our theoretical analysis, the proposed IDS scheme gives higher malicious-behavior-detection rates in certain circumstances while improving security and does not greatly affect the network performances.***

Keywords: Digital Signature, DSA,RSA, EAACK, MANET.

1. Introduction

Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. This communication is limited to the range of transmitters. MANET solves this problem by allowing intermediate parties to relay data transmissions. The nodes in the network function as routers, clients, and servers. There are two types of MANETs: closed and open. 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. However, some resources are consumed quickly as the nodes participate in the network functions.

Wireless links make MANETs more susceptible to attacks. It is easier for hackers to eavesdrop and gain access to confidential information. It is also easier for them to enter or leave a wireless network because no physical connection is required. They can also directly attack the network to delete messages, inject false packets, or impersonate a node. Nodes in MANETs are constrained in power consumption, bandwidth, and computational power. MANETs lack central administration and prior organization, so the security concerns are different than those that exist in conventional networks. Compromised nodes can also launch attacks from within a network. This violates the network's goals of availability, integrity, authentication, and nonrepudiation. As MANETs become widely used, the security issue has become one of the primary concerns. Most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious Therefore, only one compromised node can cause the failure of the entire network.

Cosidering all above cases, It is very hard task to design IDS to detect malicious node in various misbehavior activities. Many IDS work for detecting malicious node in case of misbehaving activities but failed to detect it in case of all the activites.Proposed work focus to give complete result with providing high level security to packet over unsecured wireless network.

2. Literature Survey

MANETs are the wireless networks of the mobile computing devices with no support of any fixed infrastructure. The mobile nodes use any of the radio technology like Bluetooth, IEEE 802.11 or Hiperlan for directly communicating with each other. The nodes behave as hosts as well as routers. The security challenges in the MANET arise due to its dynamic topology, vulnerable wireless link and nomadic environment. Compromised nodes can also launch attacks from within a Network [1, 2]. With the nature of mobile ad hoc networks, almost all of the intrusion detection systems (IDSs) are structured to be distributed and have a cooperative architecture. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS system itself [3, 4]. MANET network is highly dependent on the cooperation of all of its members to perform networking functions. Previous work has investigated the performance degradation

caused by such selfish (misbehaving) nodes in MANETs [5]. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches [6]. In this section, we mainly describe existing Approaches namely, Watchdog, TWOACK, Adaptive ACKnowledgment (AACK), and Enhanced Adaptive ACKnowledgment (EAACK).

Cosidering all above cases, It is very hard task to design IDS to detect malicious node in various scenarios. Many following research studies and implementations have proved that the Watchdog scheme is efficient. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme[7]. But these schemes failed 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. With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK which works on routing protocol dynamic source routing is one of the most important approaches among them in which Aiming to resolve the ambiguous collision receiver collision and limited transmission power problems of Watchdog, it detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination[8, 9]. But acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. A new scheme called AACK is introduced in which a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK) is used to significantly reduce network overhead, While maintaining or even surpassing the same network throughput[10]. But both TWOACK and AACK still suffer from the problem that they failed to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets, collusion and partial dropping. Thus new IDS called Enhanced Adaptive ACKnowledgement (EAACK) system is proposed which detects malicious node in all cases axcept in case of collusion and forged acknowledgement packet[12].Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [13]. Digital signature is a widely adopted approach to ensure the authentication, integrity, and nonrepudiation of MANETs. It can be generalized as a data string, which associates a message (in digital form) with some originating entity, or an electronic analog of a written signature [14]. With regard to this urgent concern, digital signature is incorporated in EAACK scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted [15].

3. Problem Definition

All IDS in MANET in previous methods detected malicious node in case of all misbehaving scenario such as ambiguous collision, receiver collision, limited transmission power, false misbehavior report and partial dropping except collusion, so we proposed a new method NACK Explained in proposed system in which we added two techniques namely NACK which works on collution attack. Multiple nodes in collusion can mount a more sophisticated attack. They collude to cause mischief. Because of this limitation, it may be necessary to disallow two consecutive untrusted nodes in a routing path. The proposed method detects malicious node in all above misbehaviong activities along with it, it provides high level of packet security using combination of DSA and RSA cryptography method which makes the proposed IDS system ideal for MANET.

4. Proposed Method

In NACK which consist of four major parts, namely, ACK, secure ACK (S-ACK), NACK and misbehavior report authentication (MRA), we introduced two new schemes namely NACK and the combination of DSA and RSA cryptography. Figure 4.1 presents a flowchart describing the NACK scheme.

The following assumptions are considered for the developed method, called NACK:

- We have a multi-hop ad hoc network of N nodes connected with bidirectional links.
- DSR is the protocol used for network layer.
- Each node has a unique ID and cannot be spoofed.
- In this report, a misbehavior node is defined as a node that cooperates in route finding phase and forwards all control packets (such as route request, route error, route reply, ACK) correctly, but silently drops all the data packets. Any node in the route may be misbehavior except the source and the destination nodes which are assumed to be trusted. Both the source node and the destination node are not malicious.

In order to distinguish different packet types in different schemes, we included a 3-b packet header in NACK. According to the Internet draft of DSR , there is 6 b reserved in the DSR header. In NACK, we use 4 b of the 6 b to flag different types of packets. Details are listed in Table 4.1.

Table 4.1

Packet Type Indicators	
Packet Type	Packet Flag
General Data	0000
ACK	0001
S-ACK	0010
NACK	0100
MRA	1000

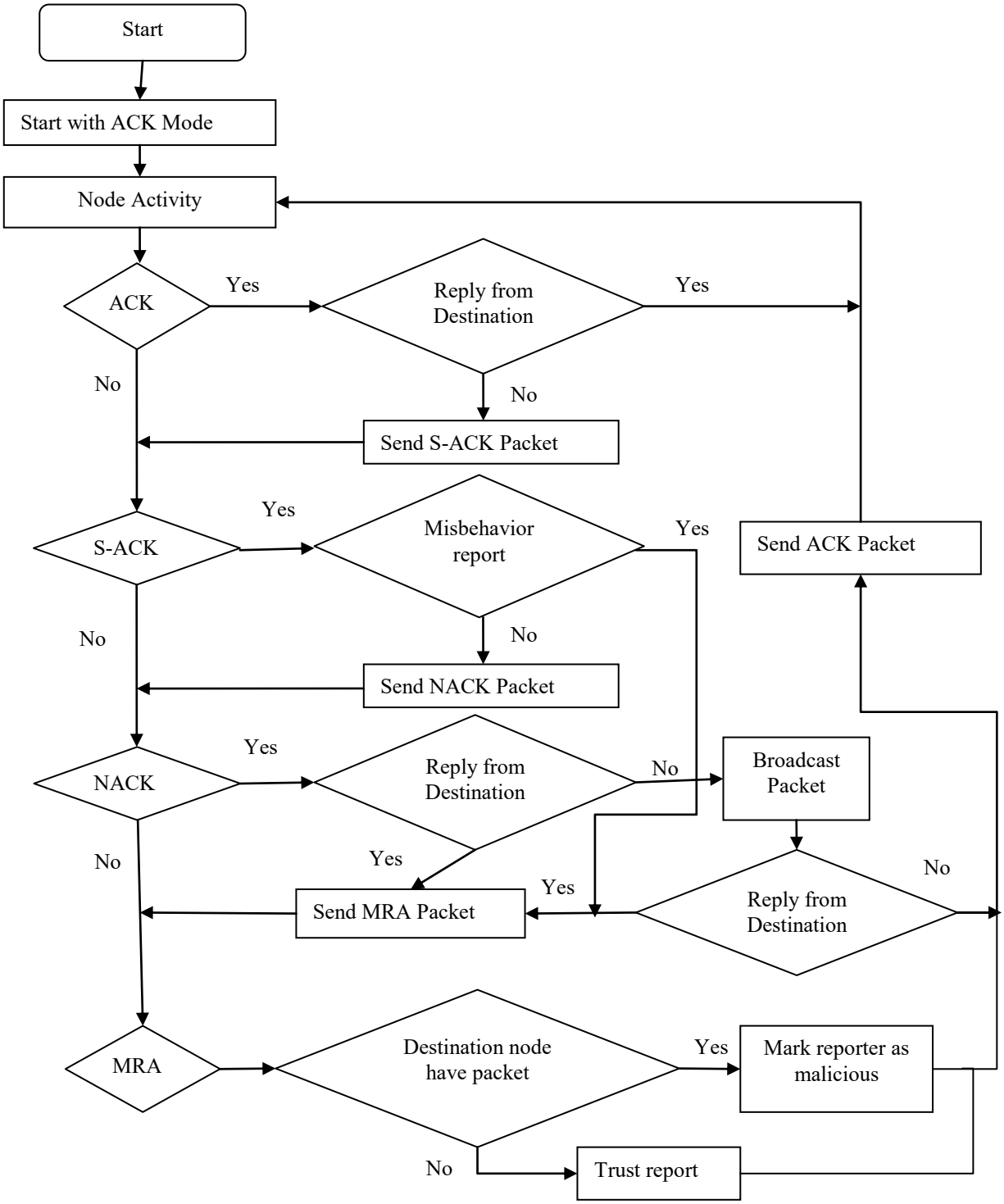

Figure 4.1: System control flow NACK scheme.

4.1 ACK

As discussed before ACK is end to end acknowledgement scheme.In ACK mode, source node S first sends out an ACK data packet *Pad*1 to the destination node D. Node D is required to send back an ACK acknowledgment packet *Pak*1 along the same route but in a reverse order. Within a predefined time period, if node S receives *Pak*1, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

4.2. S-ACK

The S-ACK scheme 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. If first node does not receive this acknowledgment packet within a predefined time period, both next nodes are reported as malicious. Moreover, a misbehavior report will be generated by node C and sent to the source node S. NACK requires the source node to switch to MRA mode and confirm this misbehavior report.

4.3. NACK

Suppose the source node selects route P for the packet forwarding to the destination node, which contains a set of Misbehavior nodes. These misbehavior nodes, placed on P, forward the control packets, but drop all data packets. If S is sending some packets to D through P = {S, n1, n2, n3, n4, D}. But, node n3 is a misbehavior node and drops the entire data packets passing through it. The goal of NACK is identifying and removing n3 from P and reporting this misbehavior node to the other nodes for isolating it by not using it for packet forwarding.

Algorithm utilized by Mobile Node

```
While ( true ) do
   Read Data Packet;
   Process it;
   If ( node is destination node ) then
      Send NACK packet to previous node
   Else
      Start timer for PckID and wait for NACK packet to be
received
      If ( NACK packet received in time)
         If ( PckID in NACK is in list)
            Remove PckID and its timer from list
            Send NACK to previous node
         End
      Else
         Send PckID Data Packet to all neighbors and start
timer and wait
            Receive ACK from neighbor
         If ( NACK packet is from next node )
            Remove PckID and its timer from list
            Send NACK to previous node
         Else
            Report next node as malicious node
 End while.
```

4.4. MRA

The MRA scheme works to detect misbehaving nodes with the presence of false misbehavior report which can be generated by malicious attackers to falsely report innocent 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.

4.5 Encryption Algorithm

In proposed work all acknowledgment packets described in this research are required to use combination of DSA and RSA cryptography at sender as well as receiver side.

4.5.1 Sender Side Algorithm

I. Key Generation Algorithm

1. Choose two distinct large prime numbers p and q.
2. Compute n= p q, where n is used as the modulus for both the public and private keys
3. Compute the totient function: $\phi(n) = (p-1)(q-1)$
4. Choose an integer e such that $1< e < \phi(n)$, and e and $\phi(n)$ share no factors other than one, where e is released as the public key exponent.
5. Compute d to satisfy the relation d * e = 1 modulus $\phi(n)$; d is kept as the private key exponent
6. The public key is (n , e) and the private key is (n , d). Keep all the values d, p, q and p secret.

II. Encryption Algorithm

7. Calculate cipher text as C=P^e (mod n).

III. Digital Signing Algorithm:

8. Create a message digest of the information to be sent by using hash function.
9. Uses her private key (n , d) to compute the signature, $s1=m^d \bmod n$.
10. Sends this signature s to the recipient B.

4.5.2 Receiver Side Algorithm

1. Receiver receives the original Message, Message Signature s1, Public-Private key pair.
2. Decrypt the message by its private key. $P = C^d \pmod n$.
3. Uses private key (n , d) to compute the signature, $s2 = m_d \bmod n$.
4. Match s1 and s2 then accept the message otherwise discard message.

4.5.3 Hash Function

1. Declare character ~~–~~str" of unsigned long type.
2. Declare and initialize hash of unsigned integer type
3. Unsigned int hash = 0;

```
int q;
while ( q= str+1)
hash = hash + q;
```

4.6 Implementation Platform

To implement wireless networks simulation tools are use such as NS-2/NS-3 or Qualnet. NS-2/NS-3 are open source tools while Qualnet is licensed tool. Many researchers prefer open source simulation tool NS2 which is object oriented simulator, written in C++, with an OTcl interpreter. In proposed system the NS2 simulator is preferred for the implementation.

5. Analysis

In this section, We took various misbehavior scenario in which previous methods failed to detect the malicious node in all cases. The situations all listed in Table 5.1 in which we compared all the Intrusion Detection System with proposed IDS NACK.

Table 5.1: Analysis of IDS in MANETS

IDS name / Scenario	Watchdog	TWO-ACK	AACK	EAACK	NACK
ambiguous collisions	No	Yes	Yes	Yes	Yes
receiver collisions	No	Yes	Yes	Yes	Yes
limited transmission power	No	Yes	Yes	Yes	Yes
false misbehavior report	No	No	No	Yes	Yes
collusion	No	No	No	No	Yes
partial dropping	No	No	No	Yes	Yes
Packet security level	No	No	No	Less	High

Yes- Detects malicious node
No- not detect malicious node

6. Conclusions

We proposed an improved IDS scheme for MANETs. The theoretical analysis proves that NACK detects the malicious node in presence of collusion attack which previous method failed to detect along with detection of malicious node in all cases namely Packet-dropping attack, ambiguous collision, receiver collision, limited transmission power, false misbehavior report and partial dropping. we extended with our proposed combination of DSA and RSA cryptography scheme which assures the packets integrity by enhancing the level of encryption in network when potential attack occurs. We think that this tradeoff is worthwhile when network security is the top priority. Our proposed NACK is expected to detect malicious nodes and provide the Stronger and complex encryption technique.

References

[1] Rashid Sheikhl Mahaka Singh Chandee and Durgesh Kumar Mishra.–Security Issues in MANET: A Review"; IEEE 978-1-4244-7202-4, 2010.
[2] 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, pp. 659–666, 2012.
[3] 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, pp. 535–541, 2012.
[4] B 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] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Transactions on Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.
[6] S B. Sun, –Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.
[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, –Mitigating routing misbehavior in mobile ad hoc networks,"; in Proc. 6th Annu. Int. Conf. Mobil Comput. Netw., Boston, MA, pp. 255–265, 2000.
[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] D. Johnson and D. Maltz, –Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, ch. 5, pp. 153–181, 1996.
[10] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, –Video transmission enhancement in presence ofmisbehaving nodes inMANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.
[11] N. Kang, E. Shakshuki, and T. Sheltami, –Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, pp. 216–222, 2010.
[12] 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.
[13] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC, T-37, 1996.
[14] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, Digital Signature Standard (DSS), 2009.
[15] 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, March 2013.
[16] Wireless Communications & Networks – William Stallings, Pearson Education.

Author Profile

Aruna P Adhav is Student ofMaster of Engineering in department of Electronics And Telecommunication at Alamuri Ratnamala Institute of Engineering and Technology. A.S.Rao Nagar, Sapgaon, Shahapur, Thane, Maharashtra 400708.

Prof K T Jadhao is Faculty of department of Electronics And Telecommunication. In Alamuri Ratnamala Institute of Engineering and Technology. A.S.Rao Nagar, Sapgaon, Shahapur, Thane, Maharashtra 400708.