ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Malicious Node Detection in MANET

Sujitha.R[1], Dr.Thilagavathy.D[2]

PG scholar, Dept. of Computer Science & Engineering, Adhiyamaan engineering college, Hosur, India[1]

Professor, Dept. of Computer Science & Engineering, Adhiyamaan engineering college, Hosur, India[2]

Abstract— Mobile Ad hoc Network (MANET) is an infrastructure less network. It does not require any fixed network. Each and every node is act as a transmitter and a receiver. All the nodes in the MANET are assumed as working within a cooperative and friendly network context. There is no base station to control the moving devices. So there is no security to protect the nodes. Any node can act as a misbehaving node. Such uncooperative behavior can greatly degrade network performance and may even result in total communication breakdown. So the malicious nodes can easily attack the mobile nodes. In this paper, we have proposed an Intrusion Detection System in which the malicious nodes are detected and there by the performance of the network will be increased.

Keywords— Enhanced Adaptive Acknowledgment (EAACK), Mobile Ad hoc Network (MANET), Intrusion Detection System(IDS).

I.INTRODUCTION

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self- configuring network of mobile devices connected by wireless links. In other words, a MANET is a collection of communication nodes that wish to communicate with each other, but has no fixed infrastructure and no predetermined topology of wireless links. Each node in a MANET [1] is free to move independently in any direction, and will therefore change its links to other devices frequently. Individual nodes are responsible for dynamically discovering other nodes that they can directly communicate with. Due to the limitation of signal transmission range in each node, not all nodes can directly communicate with each other. Each node must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET [10] is equipping each device to continuously maintain the information required to properly route traffic. Therefore, nodes are required to relay packets on behalf of other nodes in order to deliver data across the network. Two types of networks are there, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. Because of MANET's distributed architecture and changing topology, a conventional centralized monitoring technique is no longer feasible in MANETs. In such case, it is vital to develop an intrusion detection system (IDS)[1][2] specially designed for MANETs. An intrusion detection system is used to detect malicious behaviors of nodes that can compromise the security and trust of a computer system. To address this problem, IDS should be added to enhance the security level of MANETs.

II. BACKGROUND

Intrusion Detection is the problem of identifying individuals who are using a computer system without authorization and those who have legitimate access to the system but are abusing their privileges. Many intrusion detection systems have been proposed in traditional wired networks, where all traffic must go through switches, routers, or gateways. The existing methods are watchdog [7], TWOACK [6], Adaptive Acknowledgement (AACK)[9].

(a) Watchdog: The watchdog [7] identifies misbehaving nodes, while the path rater avoids routing packets through these nodes. When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next node's transmissions. If the next node does not forward the packet, then it is

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

misbehaving. The watchdog method detects misbehaving nodes.

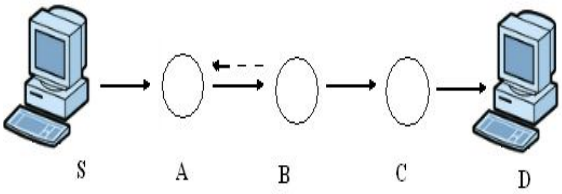

Figure 1: watchdog scheme

Figure1 illustrates how the watchdog works. Node A cannot transmit all the way to node C, but it can listen in on node B's traffic. Thus, when A transmits a packet for B to forward to C, A can often tell if B transmits the packet. If encryption is not performed separately for each link, which can be expensive, then A can also tell if B has tampered with the payload or the header. We implement the watchdog by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If the packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehavior, 5) collusion, and 6) partial dropping.

(b) TWOACK: The TWOACK[6] scheme can be implemented on top of any source routing protocol such as DSR. This follows from the fact that a TWOACK packet derives its route from the source route established for the corresponding data packet. The TWOACK scheme uses a special type of acknowledgment packets called TWOACK packets, which are assigned a fixed route of two hops (or three nodes) in the direction opposite to that of data packets. Figure 2 illustrates the operational details of the TWOACK scheme. Suppose that the process of Route Discovery has already yielded a source route [$S \rightarrow N1 \rightarrow N2 \rightarrow N3 \rightarrow \cdot \cdot \cdot \rightarrow D$] from a source node S to destination node D. For instance, when $N1$ forwards a data packet to $N2$, to be forwarded on to $N3$, $N1$ has no way of knowing if the packet reached $N3$ successfully or not. Listening on the medium, would only tell $N1$ whether $N2$ is sending out the packet or not.1 However, the reception status at $N3$ is unclear to node $N1$. The possibility of collisions at both $N1$ and $N3$ makes the overhearing technique vulnerable to medium access problems and false detections. TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog.

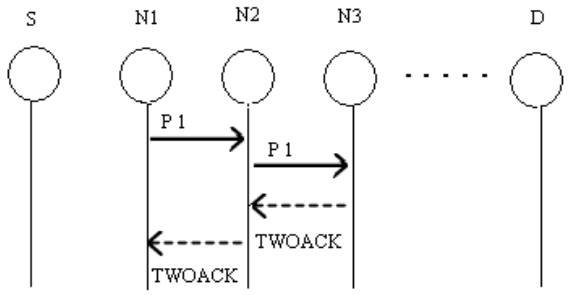

Figure 2: TWOACK scheme

However, the acknowledgement process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, Such redundant transmission process can easily degrade the life span of the entire network.

(c) AACK: Adaptive Acknowledgement (AACK)[9] is similar to TWOACK. AACK is an acknowledgement based network layer scheme which can be considered as a combination of a scheme call ACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACK. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. 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 misbehavior report and forged acknowledgement packets. In fact, many of the existing IDSs in MANETs adopt acknowledgement based scheme, including TWOACK and AACK. The function of such detection schemes all largely depend on

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

the acknowledgement packets. Hence, it is crucial to guarantee the acknowledgement packets are valid authentic. To address this concern, we adopt digital signature in proposed scheme EAACK.

III. PROPOSED SCHEME

In this section we will briefly describe about EAACK. In this paper, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgment packets. The three parts of EAACK are Acknowledgement scheme (ACK), Secure Acknowledgement (SACK), Misbehavior Report Authentication (MRA).

(i) ACK: ACK[1] is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected.

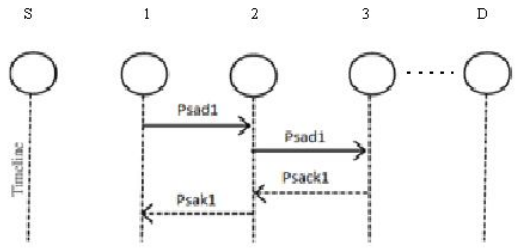

Figure 3: ACK scheme

In Figure 3, node S first sends out an ACK data packet p1 to the destination node D. If all the intermediate nodes along the route between node S and node D are cooperative and node D successfully receives p1, node D is required to send back an ACK acknowledgement packet ack1 along the same route but in a reverse order. Within a predefined time period, if node S receives ack1, 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.

(ii) SACK: The S-ACK scheme [1] 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. As shown in Figure. 3, in S-ACK mode, the three consecutive nodes (i.e., 1, 2, and 3) work in a group to detect misbehaving nodes in the network. Node 1 first sends out S-ACK data packet *Psad*1 to node 2. Then, node 2 forwards this packet to node 3. When node 3 receives *Psad*1, as it is the third node in this three-node group, node 3 is required to send back an S-ACK acknowledgment packet *Psak*1 to node 2. Node 2 forwards *Psak*1 back to node 1. If node 1 does not receive this acknowledgment packet within a predefined time period, both nodes 2 and 3 are reported as malicious. Moreover, a misbehavior report will be generated by node N1 and sent to the source node S.

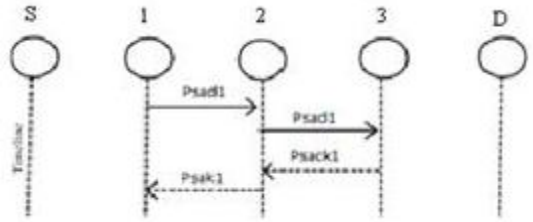

Figure 4: SACK scheme

(iii) MRA: The Misbehavior Report Authentication (MRA)[1] scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. False misbehavior report can be generated by malicious attackers to falsely report that 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 core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is none other 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, we circumvent the misbehavior reporter node. When the destination node receives an
MRA packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received, then it is safe to conclude this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

(iv) Digital signature: EAACK[1][8] is an acknowledgement based IDS. All three parts of EAACK, namely: ACK, SACK and MRA are acknowledgement based detection schemes. They all rely on acknowledgement packets to detect misbehaviors in the network. Thus, it is extremely important to ensure all acknowledgement packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgement packets, all of the three schemes will be vulnerable. In order to ensure the integrity of the IDS, EAACK requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted. In our proposed system we have to provide the digital signature to all the packets which are coming from source to destination and destination to source. Thus the packets will be protected from malicious attacks.

IV. SIMULATION RESULTS

In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics.
(1)Packet delivery ratio (PDR) It is the ratio of the total number of received packets at the destination to the total number of sent packets by the source.

*(2)Routing Overhead (*RoH) This is the ratio of routing related packets in bytes (RREQ, RREP, RERR, AACK,) to the total routing and data transmissions (sent or forwarded packets) in bytes. That means the acknowledgments, alarms and switching over head is included.
We provide the malicious nodes the ability to forge acknowledgment packets. This way, malicious nodes simply drop all the packets that they receive and send back forged positive acknowledgment packets to its previous node whenever necessary. This is a common method for attackers to degrade network performance while still maintaining its reputation. We can observe that our proposed scheme EAACK outperforms TWOACK and AACK.

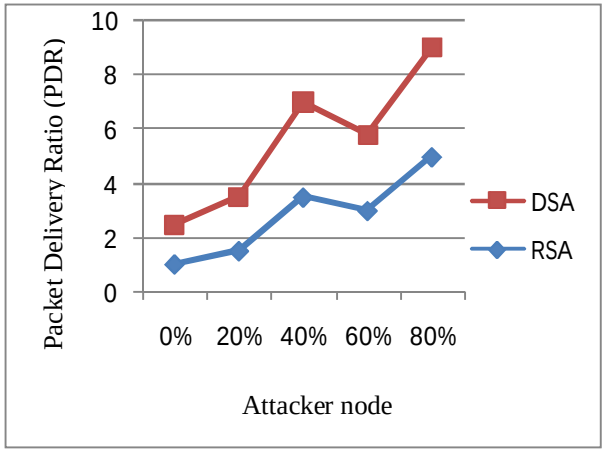

Figure 5: Packet Delivery Ratio

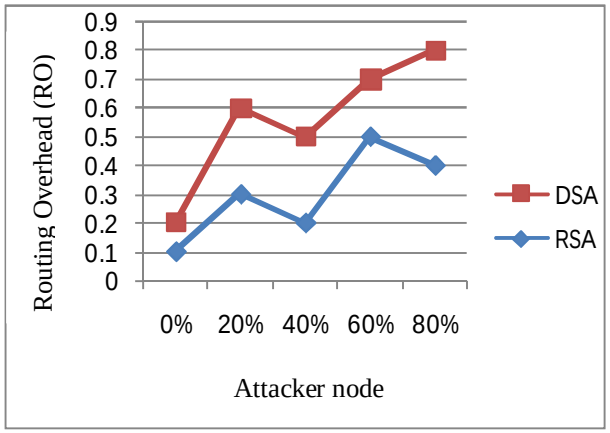

Figure 6: Routing Overhead

We believe that this is because EAACK is the only scheme which is capable of detecting forged acknowledgment packets. Regardless of different digital signature schemes adopted in EAACK, it produces more network overhead than AACK and TWOACK. We conclude that the reason is that digital signature scheme brings in more overhead than the other two schemes. So, all the packets are digitally signed by the source and destination to avoid the malicious nodes in the network. Thus the packet droppers are identified and the performance of the network has been increased.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

V. CONCLUSION AND FUTURE WORK

In this paper we have discussed about a new intrusion detection system named EAACK. We have compared and implemented both DSA and RSA schemes. Then the DSA scheme is more suitable to be implemented in MANETs when compared with RSA scheme. So, all the packets will be digitally signed by the nodes to avoid the malicious attacks. Future work is to test the performance of IDS in real network environment instead of software simulation.

REFERENCES

1. Elhadi M. Shakshuki, *Senior Member, IEEE*, 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.

2. 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.

3. 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.

4. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10, 2010, pp. 216–222.

5. 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.

6. 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.

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. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265.

8. 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.

9. 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.

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