ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Advanced Secure System For Manet

Sujitha.R[*1], Dr.Thilagavathy.D[2]
[*1]PG Scholar, [2]Professor, Computer Science & Engineering, Adhiyamaan College of engineering, Hosur, India
suji.it88@gmail.com

Abstract

Mobile Ad Hoc Networks (MANETs) are fundamentally different from their wired-side counterparts. MANETs provide no fixed infrastructure, base stations or switching centers. So there is no security to protect the nodes in the network. Each and every nodes act as a sender and receiver. Each node helps each other to perform network functions in a self organization way. However, some nodes in a network may oppose to cooperating with others to avoid consuming their battery power and other resources. So we propose and implement a new Intrusion detection system called Enhanced Adaptive Acknowledgement (EAACK). EAACK identifies the malicious nodes and improving the performance of the network.

Keywords: Mobile Ad Hoc Network (MANET), Enhanced Adaptive Acknowledgement (EAACK), Digital Signature Algorithm (DSA).

Introduction

MANET is a type of ad-hoc network in which the mobile nodes can communicate with each other when they are both within the same communication range. A mobile ad-hoc network of mobile routers (and associated hosts) connected by wireless links- the union of which form a random topology. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion or may be connected to the larger internet [4].Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations etc. Each node will be able to communicate directly with any other node that resides within the transmission range. For communication with nodes that reside beyond this range the node needs to use intermediate nodes to relay the messages hop by hop. Wireless network are adapted to enable mobility. There are two variations of mobile network. The first is infra-structured network (i.e. a network with fixed and wired gateways). The bridges of the network are known as base stations. A mobile unit within the network connects to and communicates with the nearest base station (i.e. within the communication radius). Application of this network includes office WLAN. The second type of network is infrastructure less mobile network commonly known as AD-HOC network. They have no fixed routers. There are two types of MANETs are there. They are single hop networks and multihop networks. In single hop network the nodes can communicate within the same range. In multihop network if the destination is out of radio range the source should rely on the other intermediate nodes to transmit.

Background

Intrusion Detection System

In recent years, the use of mobile ad hoc networks (MANETs) has been widespread in many applications, including some mission critical applications, and as such security has become one of the major concerns in MANETs. Due to some unique characteristics of MANETs, prevention methods alone are not sufficient to make them secure; therefore, detection should be added as another defense before an attacker can breach the system. In general, the intrusion detection techniques for traditional wireless networks are not well suited for MANETs [15]. Many intrusion detection systems have been proposed in traditional wired networks, where all traffic must go through switches, routers, or gateways. Hence, IDS can be added to and implemented in these devices easily. On the other hand, MANETs do not have such devices. Moreover, the medium is wide open, so both legitimate and malicious users can access it. Furthermore, there is no clear separation between normal and unusual activities in a mobile environment. Since nodes can move arbitrarily, false routing information could be from a compromised node or a node that has outdated

ISSN: 2277-9655
Impact Factor: 1.852

information. Thus, the current IDS techniques on wired networks cannot be applied directly to MANETs. The existing techniques are watchdog [11],TWOACK [10], and Adaptive Acknowledgement (AACK)[14].

(i) Watchdog: The watchdog [11] method allows detecting misbehaving nodes. When a node forwards a packet, the watchdog set in the node ensures that the next node in the path also forwards the packet. The watchdog does this by listening to all nodes within transmission range promiscuously. If the next node does not forward the packet then it is tagged as misbehaved. A match confirms that the packet has been successfully forwarded, causing the neighbor's trust worthiness to be increased. If a packet is not forwarded within a timeout period, then a failure tally for the node responsible for forwarding the packet is incremented. If this tally exceeds a predetermined threshold, then the node is termed as malicious. Due to the effectiveness of the watchdog and its relative easy implementation, several proposals use it as the basis of their IDS solutions. Therefore, we can find in the literature several approaches that are watchdog-based.

The watchdog methodology requires sniffing enough data packets to decide whether a node is an attacker. This means that more time is needed to make a decision compared to a network without a tolerance threshold. If the attacker is moving, there is a possibility that the malicious node moves outside the watchdog signal range, and thus it would not be detected. Therefore, false negatives can appear, and both intermittent and temporal attacks may remain undetected. The second problem is how a watchdog can determine whether a neighbor is in range or not. As we remarked before, the watchdog has the advantage of using only local information, but this has also some disadvantages, such as the watchdog does not knows when a neighbor goes out of range. This problem is solved by using timeouts: when the time that passes after the last neighbor packet listened surpasses a certain value, the watchdog considers this neighbor to be out of range and will not consider it for future tests. The main problem of this strategy is how to find the best timeout. A low value forces the watchdog to restart all calculations for a neighbor before a decision about it being malicious or not is made, possibly not detecting a malicious node, thus causing false negatives. A high value causes that, when a neighbor goes out of range, the watchdog would consider it to be in range for a long time. In that case, the watchdog would expect retransmissions from this neighbor, but would not listen to any. As a consequence, it would decide that this neighbor is a malicious node, thus causing false positives. 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.

(ii)TWOACK: TWOACK [10] is neither an enhancement nor a Watchdog based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR).

The 2ACK scheme is a network-layer technique to detect misbehaving links and to mitigate their effects. It can be implemented as an add-on to existing routing protocols for MANETs, such as DSR. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes), in the opposite direction of the data traffic route.

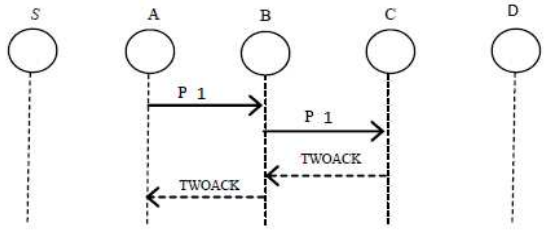


Figure: 1 TWOACK Scheme

(iii)AACK: It is based on TWOACK Acknowledgement (AACK) [14] 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

ISSN: 2277-9655
Impact Factor: 1.852

based scheme, including TWOACK and AACK. The function of such detection schemes all largely depend on 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.

Proposed Scheme

In this section we will briefly describe about EAACK in detail. 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 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. In figure 2, 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.

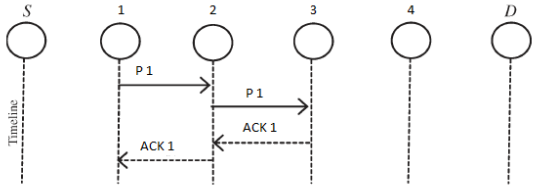


Figure 2: ACK Scheme

(ii) SACK: The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu *et al.* [10]. 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 Fig. 3, in S-ACK mode, the three consecutive nodes (i.e., N1, N2, and N3) work in a group to detect misbehaving nodes in the network. Node N1 first sends out S-ACK data packet *Psad*1 to node N2. Then, node N2 forwards this packet to node N3. When node N3 receives *Psad*1, as it is the third node in this three-node group, node N3 is required to send back an S-ACK acknowledgment packet *Psak*1 to node N2. Node N2 forwards *Psak*1 back to node N1. If node N1 does not receive this acknowledgment packet within a predefined time period, both nodes N2 and N3 are reported as malicious. Moreover, a misbehavior report will be generated by node N1 and sent to the source node S.

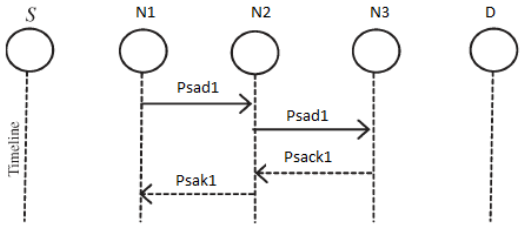


Figure 3: SACK Scheme

(iii) MRA: The Misbehavior Report Authentication (MRA) 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 scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

(iv) Digital signature: EAACK 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

ISSN: 2277-9655
Impact Factor: 1.852

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. With regarding to this urgent concern, [1] incorporated digital signature in their proposed scheme. 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.

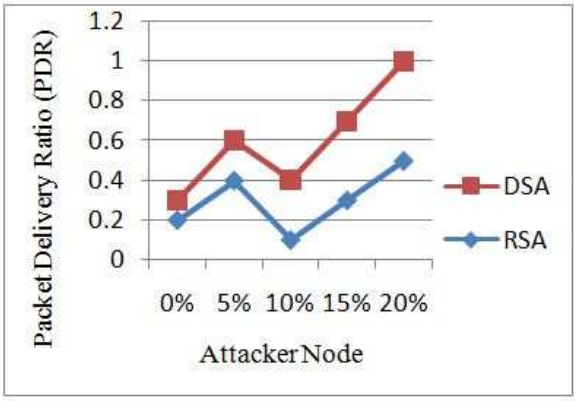
Simulation Results

In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics [13].

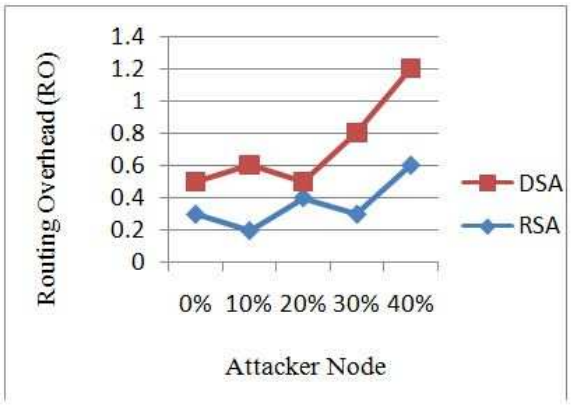
Scenario 1) *Packet delivery ratio (PDR)*: PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

Scenario 2) *Routing overhead (RO)*: RO defines the ratio of the amount of routing-related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].

During the simulation, the source route broadcasts an RREQ message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocols like DSR, a RERR message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message.



Scenario 1: Packet delivery ratio



Scenario 2: Routing overhead

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 conclusion is that the DSA scheme is more suitable to be implemented in MANETs when compared to RSA scheme. Our 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] *Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.*

[3] *Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.*

[4] *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.*

[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. 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.*

ISSN: 2277-9655
Impact Factor: 1.852

[7] 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.

[8] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.

[9] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[10] 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.

[11] 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.

[12] [12] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC, 1996, T-37.

[13] 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.

[14] 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.

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