ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

# Acknowledgment-Based Secure Authentication Method for Manet

Dr.J.Subash Chandra Bose[1], U.Akila Devi[2], M.Prasanalaxmi[3], K.Malathi[4], K.P.Vinodhini[5], S.Saranya[6]

Professor and Head, Department of Computer Science Engineering, Professional Group of Institutions, Palladam, Tamilnadu, India[1]

Assistant professor, Department of Computer Science Engineering, Professional Group of Institutions, Palladam, Tamilnadu, India[2]

Final year student, Department of Computer Science Engineering, Professional Group of Institutions, Palladam, Tamilnadu, India[3, 4, 5, 6]

**ABSTRACT:** The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. 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. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. In this paper, we added an additional feature (multiple keys) for encryption and decryption along with Digital signature. To adjust to such trend, we strongly believe that it is vital to address its potential security issues.

**KEYWORDS:** Digital signature, digital signature algorithm (DSA), Advanced Encryption Standard(AES), Enhanced Adaptive ACKnowledgment (AACK) (EAACK), Mobile Ad hoc NETwork (MANET).

## I. 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. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations.

IDS in MANETs

Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK and Adaptive ACKnowledgment (AACK).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

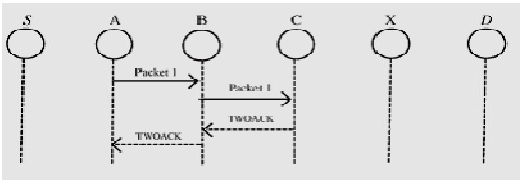
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

1) Watchdog

Marti *et al.* proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as an IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field. 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.

2) TWOACK:

With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu *et al.* is one of the most important approaches among them. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The




TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment 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. However, many research studies are working in energy harvesting to deal with this problem.

3) AACK:

Based on TWOACK, Sheltami *et al.* proposed 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. In the ACK scheme, the source node S sends out Packet 1 without any overhead except 2 b of flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1.

## II. DIGITAL SIGNATURE

Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and non-repudiation. Digital signature schemes can be mainly divided into the following two categories.

1) *Digital signature with appendix*: The original message is required in the signature verification algorithm. It include a digital signature algorithm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

2) *Digital signature with message recovery*: This type of scheme does not require any other information besides the signature itself in the verification process. A This process can be described as $H(m) = d$. The result is a signature *Sig* Alice, which is attached to message *m* and Alice's secret private key $S_{Pr-Alice}(d) = Sig_{\text{Alice}}$.

## III. COMPARISON WITH OVERHEARING TECHNIQUES

The 2ACK scheme solves the problems of ambiguous collisions, receiver collisions, and limited transmission power:

Ambiguous Collisions: Ambiguous collisions may occur at node N1. When a well-behaved node N2 forwards the data packet toward N3, it is possible that N1 cannot overhear the transmission due to another concurrent transmission in N1's neighborhood. The 2ACK technique solves this problem by requiring N3 to send a 2ACK packet explicitly

Receiver Collisions: Receiver collisions take place in the overhearing techniques when N1 overhears the data packet being forwarded by N2, but N3 fails to receive the packet due to collisions in its neighborhood. A misbehaving N2 will not retransmit the data packet, which costs extra energy. Again, the 2ACK technique overcomes this problem due to the explicit 2ACK packets.

Limited Transmission Power: A misbehaving N2 may maneuver its transmission power such that N1 can overhear its transmission but N3 cannot. This problem is similar to the Receiver Collisions problem. It becomes a threat only when the distance between N1 and N2 is less than that between N2 and N3. The 2ACK scheme is immune to limited transmission power problem.

Limited Overhearing Range: A well-behaved N2 may use low transmission power to send data toward N3. Due to N1's limited overhearing range, it will not overhear the transmission successfully and will thus infer that N2 is misbehaving, causing a false alarm.

## IV. ADAPTIVE ACKNOWLEDGMENT

*Credit-Based Schemes*

The basic idea of *credit-based* schemes is to provide incentives for nodes to faithfully perform networking functions. When they request other nodes to help them for packet forwarding. Each intermediate node earns nuggets in return for forwarding the packet.

*Reputation-Based Schemes:* Nodes operate in a promiscuous mode wherein, the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet. At the same time, it maintains a buffer of recently sent packets. A data packet is cleared from the buffer when the watchdog overhears the same packet being forwarded by the next-hop node over the medium.

*End-to-end Acknowledgment Schemes:* End-to-end acknowledgment is employed. Such acknowledgments are sent by the end-receiver to notify the sender about the reception of data packets up to some locations of the continuous data stream. The Selective Acknowledgment (SACK) technique is used to acknowledge out-of-order data blocks. The 2ACK technique differs from the ACK and the SACK schemes in the TCP protocol in the following manner: the 2ACK scheme tries to detect those misbehaving nodes which have agreed to forward data packets for the source node but refuse to do so when data packets arrive TCP.

*The TWOACK and S-TWOACK Schemes:* The 2ACK and the TWOACK schemes have the following major differences: 1) the receiving node in the 2ACK scheme only sends 2ACK packets for a fraction of received data packets, while in the TWOACK scheme TWOACK packets are sent for every data packet received. Acknowledging a fraction of received data packets gives the 2ACK scheme better performance with respect to routing overhead; 2) the 2ACK scheme has an authentication mechanism to make sure that the 2ACK packets are genuine. *Authenticating the 2ACK Packets:* The problem of 2ACK packet fabrication in this subsection. Since the 2ACK packets are forwarded by an intermediate node. Without

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

proper protection, a misbehaving node N2 can simply fabricate 2ACK packets and claim that they were sent by node N3. Therefore, an authentication technique is needed in order to protect 2ACK packets from being forged.

## V. SCHEME DESCRIPTION

ACK Scheme*:* 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 ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed ACK. A ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route. Routing misbehavior can severely degrade the performance at the routing layer.

End-to-end Acknowledgment Schemes: Acknowledgments are sent by the end-receiver to notify the sender about the reception of data packets up to some locations of the continuous data stream. The Selective Acknowledgment (SACK) technique is used to acknowledge out-of-order data blocks.

The attackers (misbehaving nodes) are assumed to be capable of performing the following tasks:

- Dropping any data packet;
- Masquerading as the node that is the receiver of its next-hop link;
- Sending out fabricated ACK packets;

EAACK is an acknowledgment-based IDS all three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network.

ACK: The hybrid scheme in EAACK to reduce network overhead when no network misbehavior is detected. ACK mode, node Source node first sends out an ACK data packet $P_{ad1}$ to the destination node. If all the intermediate nodes along the route between Source node and Destination node are cooperative and receiver node receive the message successfully receives $P_{ad1}$, receiver node is required to send back an ACK acknowledgment packet $P_{ak1}$ along the same route but in a reverse order.

S-ACK*:* The three consecutive nodes (i.e., F1, F2, and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet $P_{sad1}$ to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives $P_{sad1}$, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet $P_{sak1}$ to node F2. Node F2 forwards $P_{sak1}$ back to node F1.

MRA: The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious.

## VI. PERFORMANCE EVALUATION

1) Simulation Results—*Scenario 1:* In scenario 1, malicious nodes drop all the packets that pass through it. All acknowledgment-based IDSs perform better than the Watchdog scheme. Our proposed scheme EAACK surpassed Watchdog's performance by 21% when there are 20% of malicious nodes in the network.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

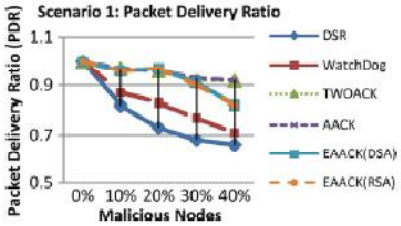
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

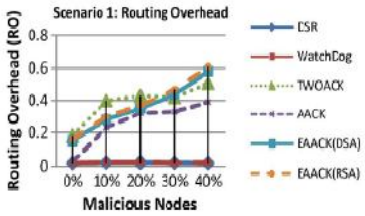
Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

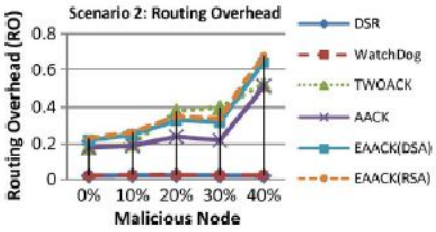



Simulation results for scenario 1—PDR.

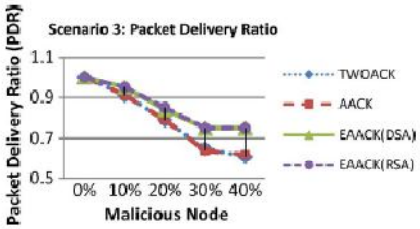



Simulation results for scenario 1—RO.

2) Simulation Results—*Scenario 2:* In the second scenario, we set all malicious nodes to send out false misbehavior report to the source node whenever it is possible. This scenario setting is designed to test the IDS's performance under the false misbehavior report. When malicious nodes are 10%, EAACK performs 2% better than AACK and TWOACK. When the malicious nodes are at 20% and 30%, EAACK outperforms all the other schemes and maintains the PDR to over 90%.




Simulation results for scenario 2—RO.




Simulation results for scenario 3—PDR.

3) Simulation Results—*Scenario 3:* In scenario 3, 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 in all test scenarios.

4) DSA and RSA: In all of the three scenarios, we witness that the DSA scheme always produces slightly less network overhead than RSA does. This is easy to understand because the signature size of DSA is much smaller than the signature size of RSA.

## VII. CONCLUSION AND FUTURE WORK

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named EAACK protocol along with multiple key generation specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, AACK and EAACK in the cases of energy, delay of packet delivery. It increases the packet delivery ratio(PDR) and security.

To increase the merits of our research work, we plan to investigate the following issues in our future research:

1) possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature.
2) Testing the performance of EAACK in real network environment instead of software simulation.

## REFERENCES

[1] *J .S. Lee*- "A Petri net design of command filters for semiautonomous mobile sensor networks".[Apr-2008]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[2] *K.Liu,J.Deng,P.K.Varshney, And K.Balakrishnan* -"An acknowledgement-based approach for the detection of routing misbehavior in MANETs".[May-2007]

[3] *S . Marti , T . J. Giuli , K . Lai ,and M . Baker*, -"Mitigating routing misbehavior in mobile ad hoc networks".[Mar-2000]

[4] *T . Sheltami , A . Al-Roubaiey , E . Shakshuki ,and A . Mahmoud*,-"Video transmission enhancement in presence of misbehaving nodes in MANETs".[Oct-2009]

[5] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard(DSS).