International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 2, Issue 3 (May-June 2014), PP. 47-52

INTRUSION IDENTIFICATION IN MANET USING ENHANCED ADAPTIVE ACKNOWLEDGEMENT

Amala Jeen A, Mohanavalli Krithika R
M.TECH CSE (Student)
SRM University
Ramapuram,Chennai

***Abstract*— A network is nothing but multiple nodes are connected with each other in some manner. The communication between each node and the topology of the network are important to make the environment more efficient. The communications between systems are broadly categorized into two; that are wired and wireless communication. In wired network, each node will be connected through physical wires and follows a topology. But in wireless network the communication between each node will be happen a centralized node called Access Point. In wireless environment a special wireless network is called MANET, in which there will be no centralized Access Points. MANET is nothing but Mobile Ad-hoc NETwork. In MANET each node acts as a sender and receiver. And there is no fixed route between nodes. Based on the nodes reachable, node will change the routing table dynamically. So the mobility and scalability of the nodes will not impact the MANET. The self-configuring ability of the MANET made it popular in military applications and emergency recovery. So the communication between each node should be more secure and trustable. And it's important to identify the malicious nodes in MANET too. The malicious nodes are nodes which are not able to sends packets further or the nodes which are sends false report to the sender. To identify these malicious nodes and sends the messages with more secure with authorization need to implement new Intrusion Identification System called Digital Signature with Acknowledgement name as Enhanced Adaptive Acknowledgement. The objective of MANET is fast communication. So its need to analyze the network throughput also once the new Intrusion Identification System introduced.**

***Key words*— Digital signature, digital signature algorithm (DSA), Enhanced Adaptive Acknowledgment, Mobile Ad hoc NETwork (MANET), Rivest Shamir Adleman (RSA), Advanced Encryption Standard (AES), Pathrater.**

I. INTRODUCTION

By definition, 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. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. 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 multi-hop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multi-hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In traditional wireless network like MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move

randomly. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. 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. Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes, so attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system specially designed for MANETs.

II. BACKGROUND

A. Instruction Identification 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. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, Intrusion Identification System should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. Intrusion

Identification System usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK, and Adaptive Acknowledgment.

1) Watchdog

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 IDS for MANETs. It is responsible for detecting malicious node misbehaviours in the network. Watchdog detects malicious misbehaviours 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. When-ever a node's failure counter exceeds a predefined threshold; the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog. Watchdog scheme fails to detect malicious misbehaviours with the presence of the following:

1) Ambiguous collisions
2) Receiver collisions
3) Limited transmission power;
4) False misbehaviour report;
5) Collision
6) Partial dropping.

2) TWOACK

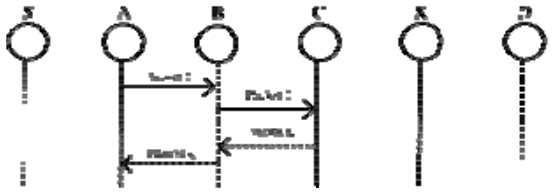

Fig. 1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

TWOACK 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 packet transmitted over every 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 acknowledgment 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 working process of TWOACK is shown in Fig. 1: Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, 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 retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same process applies to every three Consecutive nodes along the rest of the route.

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

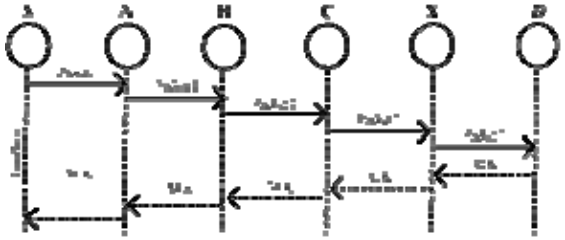

Fig. 2. ACK scheme: The destination node is required to send acknowledgment packets to the source node

In the ACK scheme shown in Fig. 2, 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, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the 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 misbehaviour report and forged acknowledgment packets.

B. Digital Signature

Fig 3. Communication using 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 pro-cesses, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and non-

repudiation. Digital signature is a widely adopted approach to ensure the authentication, integrity, and non-repudiation 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.

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. Examples include a digital signature algorithm (AES).
2. **Digital signature with message recovery:** This type of scheme does not require any other information besides the signature itself in the verification process. Examples include RSA.

Here, the digital signature is implemented using AES and RSA in Enhanced Adaptive Acknowledgement scheme. The main purpose of this implementation is to compare their performances in MANETs.

The general flow of data communication with digital signature is shown in Fig. 3. First, a fixed-length message digest is computed through a pre agreed hash function H for every message m. This process can be described as

$$H(m\_) = d\_. \qquad (3)$$

Bob can verify the signature by applying Alice's public key Pk−Alice on SigAlice, by using

$$SPk{-}Alice\ (SigAlice) = d. \qquad (4)$$

If d == d_, then it is safe to claim that the message m_ transmitted through an unsecured channel is indeed sent from Alice and the message itself is intact. Each and every communication between the source node and destination should be used this digital signature method.

III. PROBLEM DEFINITION

Our proposed approach Enhanced Adaptive Acknowledgement is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehaviour, limited transmission power, and receiver collision. In this section, we discuss these three weaknesses in detail.

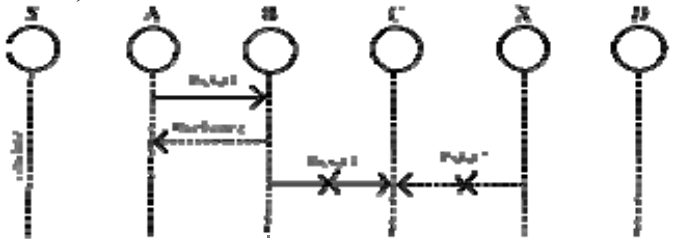

Fig. 4. Receiver collisions: Both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time.

Fig. 5. Limited transmission power: Node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

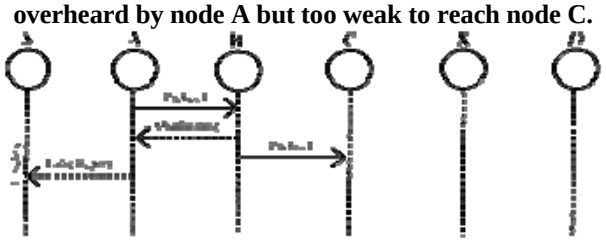

Fig. 6. False misbehaviour report: Node A sends back a misbehaviour report even though node B forwarded the packet to node C.

In a typical example of receiver collisions, shown in Fig. 4, after node a sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, node A overhears that node B has successfully forwarded Packet 1 to node C but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

In the case of limited transmission power, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C, as shown in Fig. 5.

For false misbehaviour report, although node A successfully overheard that node B forwarded Packet 1 to node C, node a still reported node B as misbehaving, as shown in Fig. 6. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehaviour report attack.

TWOACK and AACK solve two of these three weaknesses, namely, receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehaviour attack. In the proposed system, the goal is to propose new Intrusion Identification system specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehaviour problem.

IV. PROPOSED SYSTEM

Enhanced Adaptive Acknowledgement is consisted of three major parts, namely, End to End Acknowledgement (EEACK), secure TWOACK (S-TWOACK), and False Report Identification (FRI). In order to distinguish different packet types in different schemes, we included a 2-b packet header in Enhanced Adaptive Acknowledgement. According to the Internet draft of DSR, there is 6 b reserved in the DSR header. In Enhanced Adaptive Acknowledgement, we use 2 b of the 6 b to flag different types of packets. Details are listed in Table.

Packet Type	Packet Flag
General Packet	00
EEACK	01
S-TWOACK	10
FRI	11

Fig.7 presents a flowchart describing the Enhanced Adaptive Acknowledgement scheme. Please note that, in our proposed scheme, we assume that the link between each node in the

network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver.

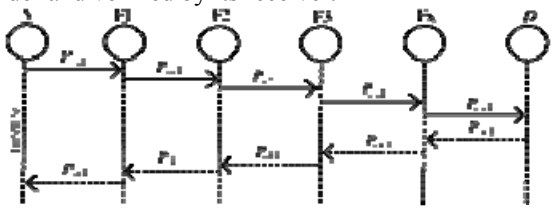

Fig. 7. System control flow: This figure shows the system flow of how the Enhanced Adaptive Acknowledge scheme works.

A. Enhanced Adaptive Acknowledge

Enhanced Adaptive Acknowledge is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in Enhanced Adaptive Acknowledgement, aiming to reduce network overhead when no network misbehaviour is detected.

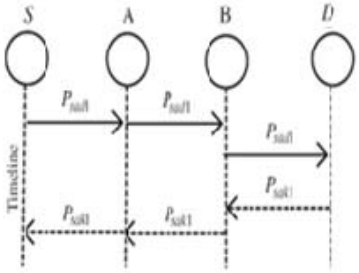

Fig. 8 EEACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

In Fig. 8, in EEACK mode, node S first sends out an EEACK data packet Pad1 to the destination node D. If all the intermediate nodes along the route between nodes S and Dare cooperative and node D successfully receives Pad1, node D is required to send back an ACK acknowledgment packet Pak1 along the same route but in a reverse order. Within a predefined time period, if node S receives Pak1, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-TWOACK mode by sending out an S-TWOACK data packet to detect the misbehaving nodes in the route.

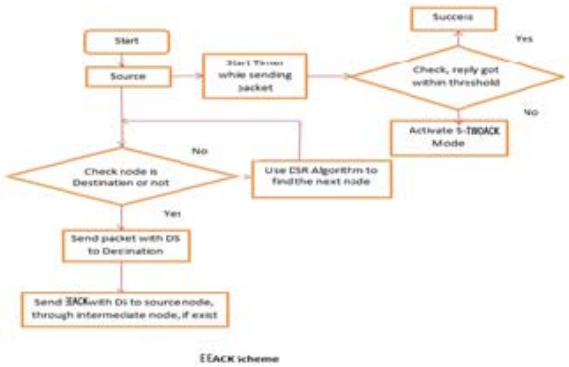

Fig 9: EEACK Scheme Flow

B. S-TWOACK

The S-TWOACK scheme is an improved version of the TWOACK. 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-TWOACK acknowledgment packet to the first node. The intention of introducing S-TWOACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

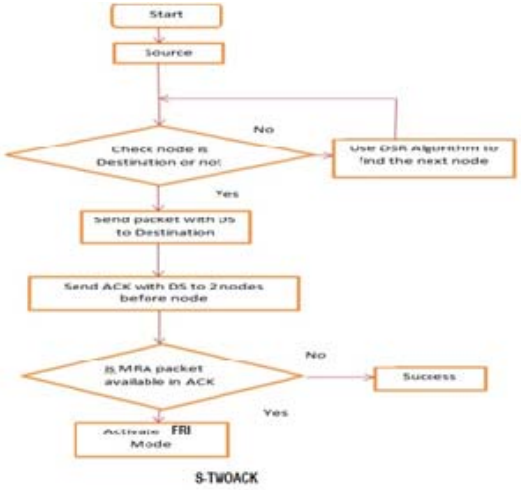

Fig 10. S-TWOACK Flow

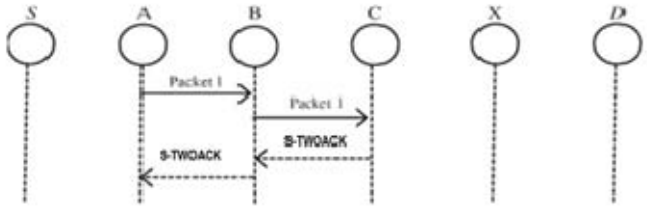

Fig. 11 S-TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

As shown in Fig. 11, in S-TWOACK mode, the three consecutive nodes (i.e., A, B, and C) work in a group to detect misbehaving nodes in the network. Node A first sends out S-ACK data packet Psad1 to node B. Then, node B forwards this packet to node C. When node F3 receives Psad1, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet Psak1 to node B. Node B forwards Psak1 back to node F1. If node A does not receive this acknowledgment packet within a predefined time period, both nodes B and C are reported as malicious. Moreover, a misbehaviour report will be generated by node A and sent to the source node S.

Nevertheless, unlike the TWOACK scheme, where the source node immediately trusts the misbehaviour report, Enhanced Adaptive Acknowledgement requires the source node to switch to FRI mode and confirm this misbehaviour report. This is a vital step to detect false misbehaviour report in our proposed scheme.

C. FRI

The FRI scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. The false misbehaviour

report can be generated by malicious attackers to falsely report 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 FRI scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

To initiate the FRI mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that 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.

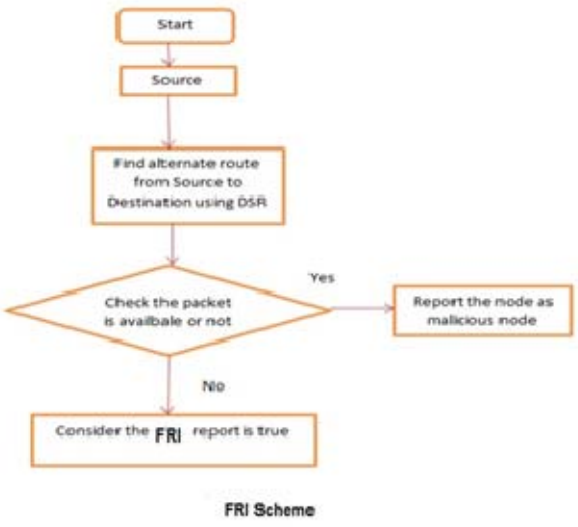

Fig 12.FRI scheme flow

By adopting an alternative route to the destination node, we circumvent the misbehaviour reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehaviour report and whoever generated this report is marked as malicious. Otherwise, the misbehaviour report is trusted and accepted.

By the adoption of FRI scheme, Enhanced Adaptive Acknowledgement scheme is capable of detecting malicious nodes despite the existence of false misbehaviour report.

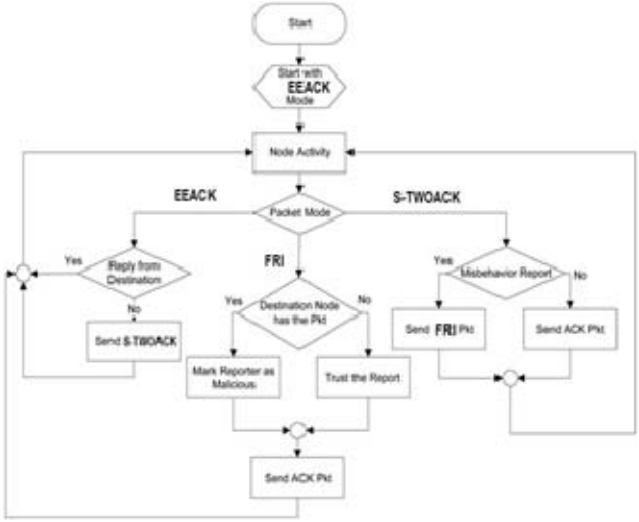

Fig.13 Overall System Flow: Enhanced Adaptive Acknowledgement scheme

D. Digital Signature

Enhanced Adaptive Acknowledgement scheme is an acknowledgment based Intrusion Identification System. All three parts of Enhanced Adaptive Acknowledgement scheme, namely, EEACK, S-TWOACK, and FRI, are acknowledgment based detection schemes. They all rely on acknowledgment packets to detect misbehaviours in the network. Thus, it is extremely important to ensure that all acknowledgment packets in Enhanced Adaptive Acknowledgement scheme are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.

In order to ensure the integrity of the Intrusion Identification System, Enhanced Adaptive Acknowledgement scheme requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented both AES and RSA digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

V. CONCLUSION

Packet dropping attack has always been a major threat to the security in MANETs. Enhanced Adaptive Acknowledge protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehaviour report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, to incorporate digital signature in our proposed scheme. It can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets. In order to seek the optimal DSAs in MANETs, we implemented both AES and RSA schemes in simulation. Eventually, the conclusion is that the DSA scheme is more suitable to be implemented in MANETs. To increase the merits to investigate the following issues in our future:

1. Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature;
2. Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of redistributed keys;
3. Testing the performance of Enhanced Adaptive Acknowledge in real network environment instead of software simulation.

VI. ACKNOWLEDGMENT

I would like to thank IJTRA members, on helping me to prepare this document by providing a template format. And I would like to thank my guide for providing her wonderful

guidance. And I would like to thank all IEEE members for their papers.

REFERENCES

[1] 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.

[2] 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, 2012, pp. 535–541.

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

[4] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002

[5] 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

[6] 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.

[7] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. WAS, Paris, France, Nov. 8–10, 2010.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

[14] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proc. ACM Workshop Wireless Secur., 2002.