RESEARCH ARTICLE OPEN ACCESS

Intrusion Detection System Using EAACK and Digital Signature For Authentication in MANET

Nithya Karthika M[1], Raj Kumar[2]
P.G Scholar[1], Assistant Professor[2]
Department of Computer Science and Engineering, Info Institute of Engineering,
Anna University, Chennai, Tamil Nadu, India

ABSTRACT
Mobile Ad hoc Network 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. 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. It is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. The proposed technique used is Enhanced Adaptive Acknowledgment for intrusion-detection system specially designed for MANETs. Digital Signature Algorithm used for obtaining a Authentication of message , Digital signature schemes can be used with two schemes are, Digital signature with appendix, Digital signature with message recovery. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead.

Keywords:- Digital signature, digital signature algorithm (DSA), Enhanced Adaptive Acknowledgment (EAACK) Mobile Ad hoc Network

I. INTRODUCTION

MANETS are wireless networks, and decentralized and no fixed topology. Each node in network act both as transmitter and receiver. Nodes communicate with each other either directly or indirectly (with the help of their neighbors).Hence this is possible by single hop network and Multi-hop networks. In Single-hop network, all the nodes within the same radio range communicate with each other. In Multi-hop network, nodes depend on neighbors to transmit if destination node is out of their radio range. MANET is highly vulnerable to attacks because, node configuration and maintenance are done on its own. Then Enhanced Adaptive ACKnowledgement scheme is used to overcome the disadvantage of false misbehaviour report. MANET are mostly preferred for military, areas that include natural disaster, medical emergency.

One of the primary concerns related to ad hoc networks is to provide a secure communication among mobile nodes in a hostile environment. The nature of mobile ad hoc networks poses a range of challenges to the security design. These include an open decentralized peer-to-peer architecture, a shared Wireless medium and a highly dynamic topology. This last point is where the main problem for MANET security resides: the ad hoc networks can be reached very easily by users, but Also by malicious attackers. If a malicious attacker reaches the network, the attacker can easily exploit or possibly even disable the mobile ad hoc network. The identities and locations of the nodes in the route, and in particular, those of the source and the destination, should be hidden and protected. Multiple paths should be established to increase the difficulty of traffic analysis and avoid broken links due to node mobility. Conventional methods of identification and authentication are not available since the availability of a Certificate Authority or a key Distribution Center cannot be assumed. In next section related work is explained, then existing system which explains Enhanced Adaptive ACKnowledgement in detail, and proposed system explains about Hybrid Cryptography Technique.

II. RELATED WORK

A. IDS in MANETs

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, an Intrusion Detection System IDS 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. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches. Anantvalee and Wu presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK, and Adaptive ACKnowledgment (AACK).

1) Watchdog

Marti 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 Path rater. 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. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission. Access to a centralized reputation authority.

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 scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it. the contrary to many other schemes, 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.

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.

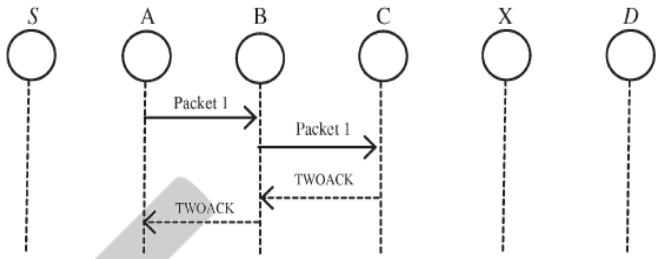

Fig.1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

The same process applies to every three consecutive nodes along the rest of the route. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead.

3) AACK

Based on TWOACK, 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. The end-to-end acknowledgment scheme in ACK is shown in Fig. 2.

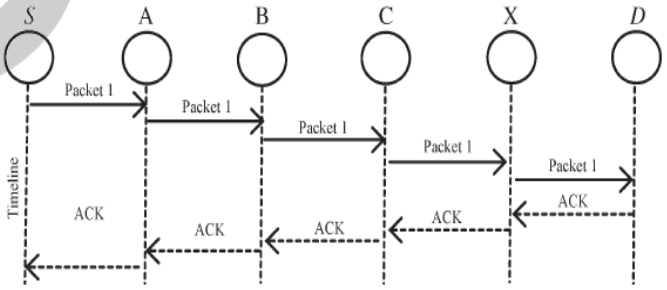

Fig. 2. ACK scheme: The destination node is required to send acknowledgment Packets to the source node.

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 misbehavior report and forged acknowledgment packets. In fact, many of the existing IDSs in MANETs adopt. To address this concern, we adopt a digital signature in our proposed scheme named Enhanced AACK (EAACK).

B. 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 [18].

The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and non repudiation [18]. 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 [33].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 (DSA) [33].

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 [23].

In this research work, we implemented both DSA and RSA in our proposed EAACK scheme. The main purpose of this implementation is to compare their performances in MANETs.

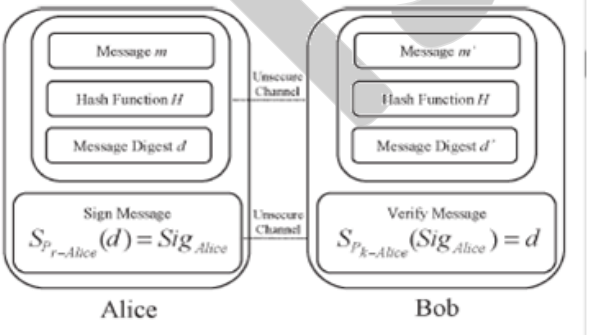

Fig.3 Communication with digital signature.

To ensure the validity of the digital signature, the sender Alice is obliged to always keep her private key Pr−Alice as a secret without revealing to anyone else. Otherwise, if the attacker Eve gets this secret private key, she can intercept the message and easily forge malicious messages with Alice's signature and send them to Bob. As these malicious messages are digitally signed by Alice, Bob sees them as legit and authentic messages from Alice. Thus, Eve can readily achieve malicious attacks to Bob or even the entire network.

III. PROPOSED SYSTEM

In our propose system, we used is Enhanced Adaptive Acknowledgment for intrusion-detection system specially designed for MANETs. Digital Signature Algorithm used for obtaining a Authentication of message , Digital signature schemes can be used with two schemes are, Digital signature with appendix, Digital signature with message recovery. The concept of adopting a hybrid scheme in AACK called as a hybrid key cryptography technique that reduce the network overhead. Network overhead increases when number of malicious node in network increases, because the count of acknowledged packet increases. Thus to reduce network overhead Hybrid key cryptography technique is used.

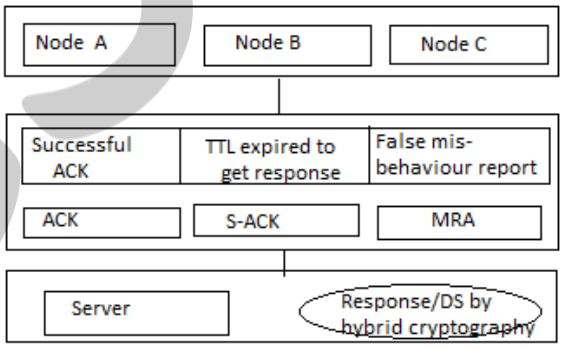

Fig.4 System Architecture

In MANETS Intrusion Detection System are installed in each and every node. Some of the basic IDS that are available are,

1. Watchdog scheme
2. Twoack scheme
3. Adaptive Acknowledgment.

These schemes are suffered with various disadvantages like receiver collision, limited power transmission problem, false misbehaviour report, ambiguous collision, and partial dropping.

A new technique called Enhanced Adaptive Acknowledgment is introduced. It solves all the three above issues. This technique depends on acknowledged packets. So it also includes Digital Signatures to prevent the attackers from attacking the packets. EAACK consist of 3 parts namely:

1. ACK
2. Secure ACK(S-ACK)
3. Misbehaviour Report Authentication (MRA).
4. Digital Signature.

A. ACK

ACK: ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected.

In ACK scheme, source node should get the acknowledgment packet within the predefined time period, it implies that destination node receives the packet and no malicious node exists in the route, otherwise send secure ACK packet.

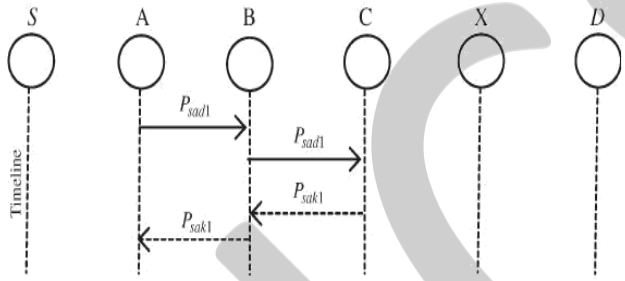

Fig. 5 ACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

B. Secure ACK(S-ACK)

SACK: The S-ACK scheme 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

The intention of introducing S-ACK mode is to find malicious node by forming every three nodes into one group. First node sends packet to next node, third node is required to send back S-ACK packet to first node otherwise second and third nodes are malicious.

C. Misbehaviour Report Authentication (MRA).

MRA: To initiate the MRA 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 two nodes. Then MRA scheme is to check whether misbehaviour report is authentic by checking that reported missing packet is received by receiver via some other route. If destination node already receives this packet then node which generates this report is marked as malicious. Otherwise false misbehaviour report is trusted and destination node is marked as malicious.

D. Digital Signature

Digital Signature is used to digitally sign the packets both at the sender and receiver side to prevent the forging of packets. Thus required resources need to be incorporated for implementing digital signature and both DSA and RSA can be used.

EAACK is an acknowledgment-based IDS. All three parts of Enhanced AACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in Enhanced AACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. With regard to this urgent concern, we incorporated digital signature in our proposed 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. 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 DSA [33] and RSA [23] digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

IV. PERFORMANCE EVALUATION

In this section, we concentrate on describing our simulation environment and methodology as well as comparing performances through simulation result comparison with Watchdog, TWOACK, and EAACK schemes.

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

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.

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.

Network Simulator 2 (NS2) is used to investigate the performance of EAACK under different types of attacks.

.A. Simulation Parameters

- Simulation time : 10 mins
- Number of nodes : 50
- Topology area : 1611m x 766 m
- Mobility model : Random way point
- Traffic type : UDP
- Maximum speed : 20 m/s
- Packet size : 512 bytes for UDP
- Propagation : Two Ray Ground
- Channel type : Wireless channel

B. Performance Analysis

The results, we conclude that acknowledgment-based schemes, including TWOACK, AACK, and EAACK, are able to detect misbehaviors with the presence of receiver collision and limited transmission power. However, when the number of malicious nodes reaches 40%, our proposed scheme EAACK's performance is lower than those of TWOACK and AACK. We generalize it as a result of the introduction of MRA scheme, when it takes too long to receive an MRA acknowledgment from the destination node that the waiting time exceeds the predefined threshold.

Here we represent three scenarios for the performance evaluation based on routing overhead. Scenario 1: To test performance of IDS against receiver collision and limited power transmission. Scenario 2: To test performance of IDS against false misbehavior report. Scenario 3: To test performance of IDS when attackers are able to forge acknowledgement packets.

DSA and RSA: This is easy to understand because the signature size of DSA is much smaller than the signature size of RSA. However, it is interesting to observe that the RO differences between RSA and DSA schemes vary with different numbers of malicious nodes. The more malicious nodes there are, the more ROs the RSA scheme produces. We assume that this is due to the fact that more malicious nodes require more acknowledgment packets, thus increasing the ratio of digital signature in the whole network overhead. With respect to this result, we find DSA as a more desirable digital signature scheme in MANETs. The reason is that data transmission in MANETs consumes the most battery power. Although the DSA scheme requires more computational power to verify than RSA, considering the tradeoff between battery power and performance, DSA is still preferable. The number of packets originated by the source at application layer to number of packets received by the destination node, which also known as the packet delivery ratio or throughput.

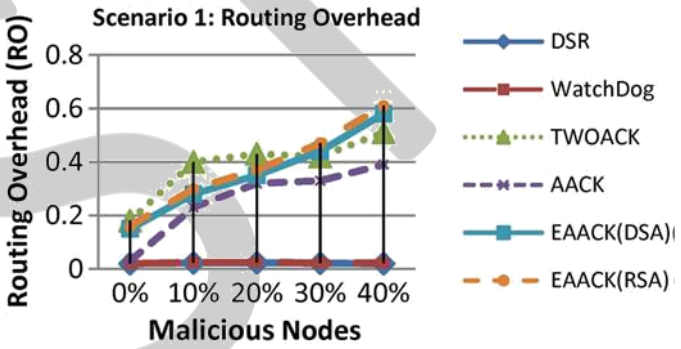

Fig 7. Simulation results for scenario 1—RO.

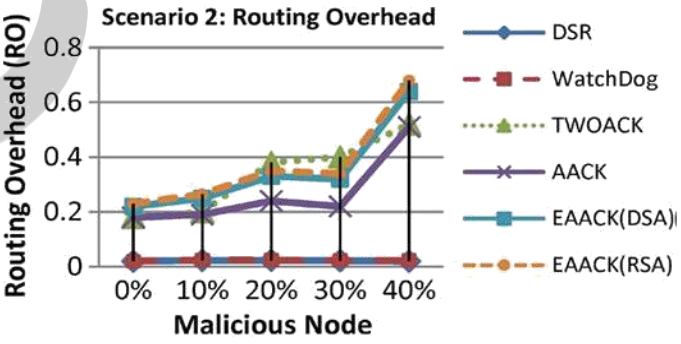

Fig 8. Simulation results for scenario 2—RO.

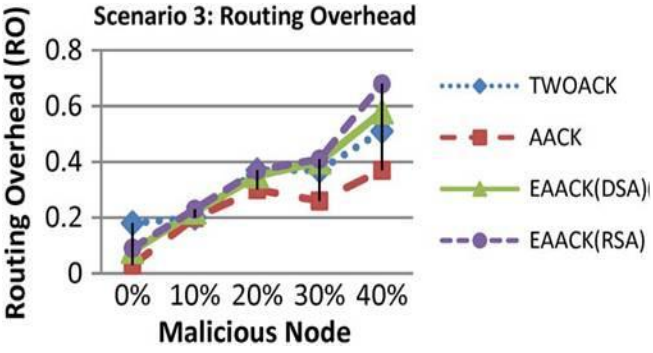

Fig 9. Simulation results for scenario 3—RO.

V. 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 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 misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate digital signature in our proposed scheme. In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs.

In future the future work: To allow the execution of EAACK scheme in real time environment to obtain accurate results for testing.

REFERENCES

[1] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[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, 2012, pp. 659–666.

[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, 2012, pp. 535–541.

[4] 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] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," IEEE Trans. Ind. Electron., 2008.

[7] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind. 2009.

[8] 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,

[9] 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, 2002.

[10] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci.,2007.

[11] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996.

[12] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, 2010.

[13] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore,2011.

[14] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const.,2004.

[15] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron.,2008.

[16] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., May 2007.

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput.2000.

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

[19] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int.2007.

[20] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detectionand response for mobile ad hoc networks," in Proc. IEEE Int. Conf.2004.

[21]] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf,2003.

[22] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in Proc.ervasive Comput. Commun., 2005.

[23] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. Feb. 1983.

[24] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros-Mendez, "Energy harvesting from piezoelectric materials fully integrated in footwear," IEEE Trans. Ind. Electron.,2010.

[25] 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.

[26] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET," in Communications in Computer and Information Science,2011.

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

[28] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," in Proc. 2nd Conf. m-Bus., Vienna,Austria, Jun. 2003.