MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

A SECURE INTRUSION DETECTION SYSTEM FOR MANETS USING EAACK

Ganesh Bhanudas Munde, Prof. Sunil Damodar Rathod

Computer Dept
Dr. D. Y. Patil School Of Engineering, (Affiliated to Savitribai Phule Pune University)
Pune, India

Abstract: *The migration to wireless network from wired network has been a global trend since the evolution of wireless network. Among all the types of wireless networks, MANET (Mobile Ad hoc NETwork) is one of the most unique and distinctive application. Unlike traditional wireless networks, MANET doesn't require a fixed infrastructure. Every single node in MANET acts as both transmitter and receiver. Nodes communicate with each other directly if they are within a communication range, otherwise they rely on their neighbor nodes to transmit messages. MANET is capable of creating a self-configuring and self-maintaining network without the need of a centralized infrastructure and this ability made it famous in mission critical use such as military or emergency. However MANETs are vulnerable malicious attacks because of open medium and its wide distribution of nodes, hence, it is crucial to develop efficient intrusion detection systems for MANET to protect it from attacks. Our proposed system named EAACK (Enhanced Adaptive ACKnowledgment) is specially designed for MANET.As compared to alternative approaches; EAACK demonstrates higher intrusion detection rates and also does not greatly affect the network performance*

Keywords*: Digital signature, digital signature algorithm (DSA), Enhanced Adaptive ACKnowledgment (EAACK), Mobile Ad hoc NETwork (MANET)*

1. INTRODUCTION

Due to the mobility and scalability they offer, Wireless networks are always preferred since the day of its invention. With rapid improvement and cut in hardware costs, wireless networks have gained much more popularity over wired networks in the past few decades. One of the major advantages of wireless networks is its ability to allow data communication between different nodes and still maintain their mobility. However, this communication is constrained by the range of transmitters. It means that two nodes cannot communicate with each other when the distance between them is beyond the communication range. MANET solves this problem by allowing intermediate parties to relay data transmissions.

By definition, a mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. It 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. MANET is divided into two types, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other where as in a multihop network nodes rely on other intermediate neighbor nodes to transmit if the destination node is out of their communication range. In contrary to the traditional wireless network, MANET does not require a fixed infrastructure and has a decentralized network infrastructure. Hence, all nodes are free to move randomly [10], [27], and [29].

MANET is capable of self-configuring and self-maintaining network without the help of a centralized infrastructure. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or when it is unfeasible to install the network infrastructure in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations [19].

However, considering the fact that MANET is becoming popular among critical mission applications, Network security is main concern in MANET. Due to open medium and remote distribution, MANET is vulnerable to malicious attacks. For example, because of the lack of physical protection of nodes, malicious attackers can easily capture and compromise nodes to achieve attacks. Also considering the fact that most routing protocol in MANETs assume that every node behaves cooperatively with other nodes in the network and assumes it's no malicious [5], attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. Hence, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANET. Many research efforts have been devoted to such research topic [1]–[3], [6]–[9], [11], [16], [24], and [29].

2. BACKGROUND

2.1 Intrusion Detection System in MANETs

As discussed in last section, due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes are always cooperate with each other to relay data and not malicious. This leaves the attackers with the opportunities to hack into the network by inserting one or more malicious or non-cooperating nodes. To address this security threat, IDS should be developed to enhance the security level of MANETs. If system can detect the attackers as soon as they enter the network, it will be able to completely eliminate the potential damages caused by compromised nodes at the first time itself. IDS act as a secondary layer in MANET and greatly complement the existing approaches. Following are existing approaches namely, Watchdog [17], TWOACK [11], and Adaptive ACKnowledgment (AACK) [25].

1. Watchdog

Watchdog serves as an ID for MANETs. This scheme aims at monitoring the activity of the nodes in the network in order to detect misbehavior. The Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. When a node forwards a packet, the watchdog

set in the node verifies that the next node in the path also forwards the packet. The watchdog does this by listening to all nodes within transmission range promiscuously. When 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 and the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

Due to the effectiveness of the watchdog and its relative easy implementation, Watchdog became a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme [11], [20], [25].However 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. Watchdog detects malicious not malicious links.

2. TWOACK

Many efforts are done to solve the above six weaknesses of watchdog. TWOACK scheme is one of the most important approaches amongst them. Unlike many others schemes TWOACK is neither enhancement nor a watchdog based system. 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 receiving of a packet, each node along the route is sends 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. 2.1.1

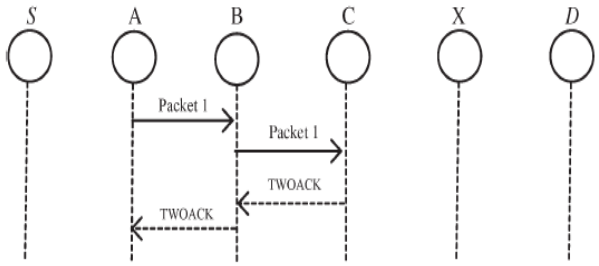

Fig. 2.1.1 TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it

Node A first forwards Packet 1 to node B, 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 has to generate a TWOACK packet, sends it back to node A via reverse route. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. 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 increases unwanted congestion in network. Due to the limited battery power of mobile nodes in MANETs, such redundant transmission process degrades the performance of network.

3. AACK

It is based on TWOACK. AACK is an Adaptive Acknowledgment-based network layer scheme which may be considered as the combination of a TACK (identical to TWOACK) and end-to-end acknowledgment scheme referred to as 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. 2.1.2

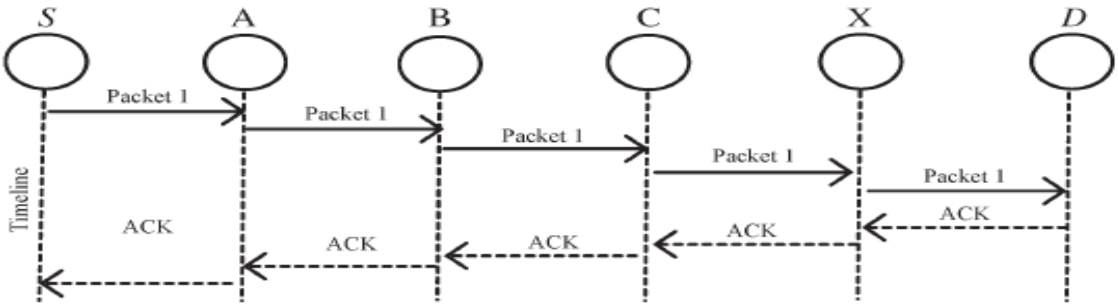

Fig. 2.1.2 ACK scheme: The destination node is required to send acknowledgment packets to the source node

In AACK, the source node S sends out Packet 1 without any overhead with a 2-bit flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it sends back an ACK acknowledgment packet to the source node S along the reverse order of the same route. If the source node S receives this ACK acknowledgment packet within a predefined time period, then the packet transmission is successful from node S to node D. If S does not receive this ACK packet, the source node S will switch to TACK scheme by sending out a TACK packet. The combination of these two schemes 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. Many of the existing IDSs in MANETs adopt this scheme but the detection scheme largely depends on the acknowledgment packets, hence it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this issue, a digital signature is adopted in our proposed scheme named Enhanced AACK (EAACK).

2.2 Digital Signature

Digital Signature has continually 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 pursuit of secure communication has been conducted by person since 4000 years ago in Egypt, and in keeping with Kahn's book in 1963. Such development dramatically accelerated since the World War II, which some believe is largely due to the globalization or economic process. The security in MANETs is outlined as a mix of processes, procedures, and systems used to ensured confidentiality, authentication, integrity, availability, and nonrepudiation. Digital signature may be a wide adopted approach to confirm the authentication, integrity, and non repudiation of MANETs.

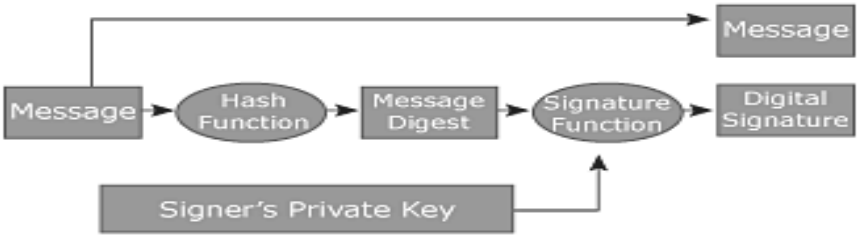

Fig.3. Communication with digital signature.

To ensure the validity of the digital signature, the message is send to the hash function or if the message is valid data means it directly send to the messages, and the hash function is processed and then it sender to the message digest, the message digest is used to check the message whether the message is valid or not. And then it sender to the signature function, it check signature is private key or public key. To verify the signature by applying public key or private key by using generalized as an information string

3. PROBLEM DEFINITION

Our proposed system EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision.

Receiver Collision

Both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time

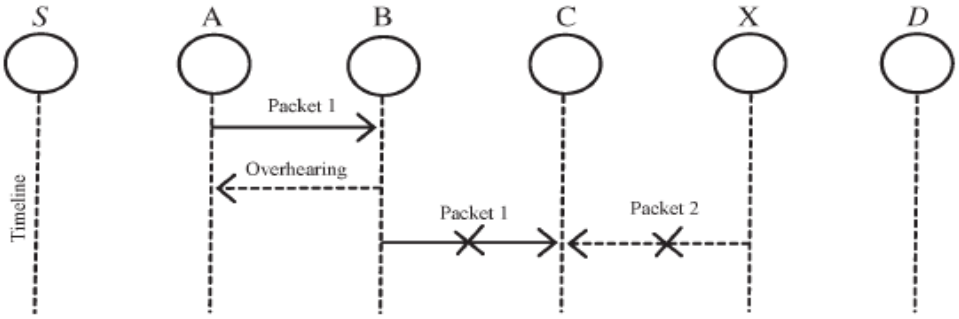

Fig. 3.1 Receiver collisions

3.1 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.

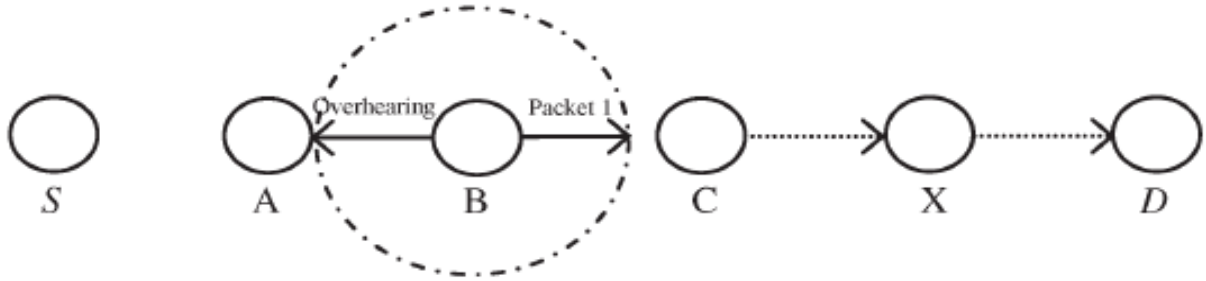

Fig. 3.2 Limited transmission power

3.2 False misbehavior report

Node A sends back a misbehavior report even though node B forwarded the packet to node C.

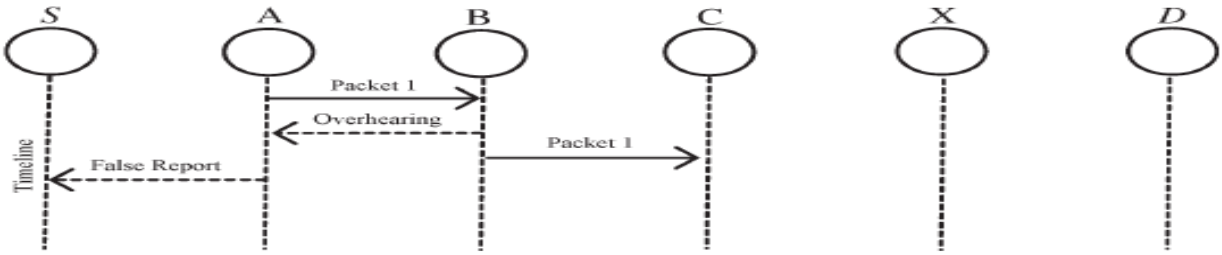

Fig. 3.3 False misbehavior report

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 misbehavior attack. In our approach, our goal is to propose new IDS specially designed for MANETs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem

4. SCHEME DESCIRPTION

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).Fig. 4.1 presents a flowchart describing the EAACK scheme

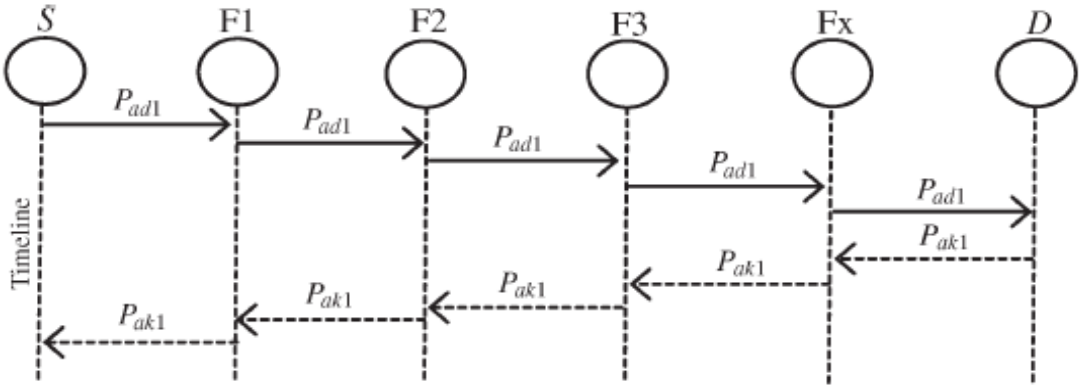

Fig. 4.1 System control flow: This figure shows the system flow of how EAACK scheme works

4.1 ACK

In ACK node S first sends out an ACK data packet Pad1 to the destination node D. If all the intermediate nodes along the route between nodes S and D are 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-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route

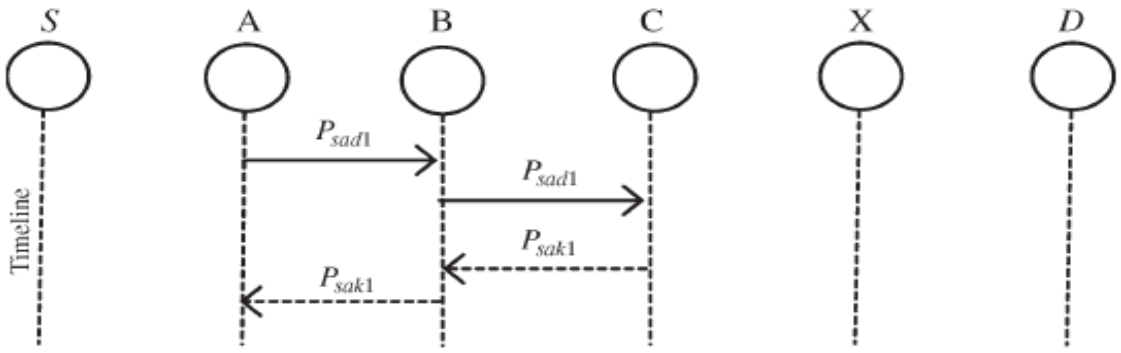

Fig. 4.1.1 ACK scheme: The destination node is required to send back an Acknowledgment packet to source node when it receives a new packet

4.2 S-ACK

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.4.2.1, in S-ACK mode, 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 Psad1 to node F2. Then, node F2 forwards this packet to node F3. 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 F2. Node F2 forwards Psak1 back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S.

Unlike the TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is an important step to detect false misbehavior report in our proposed scheme.

4.3. MRA

The false misbehavior report can be generated by malicious attackers to falsely report genuine nodes as malicious. The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

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 between two nodes.

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 misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted.

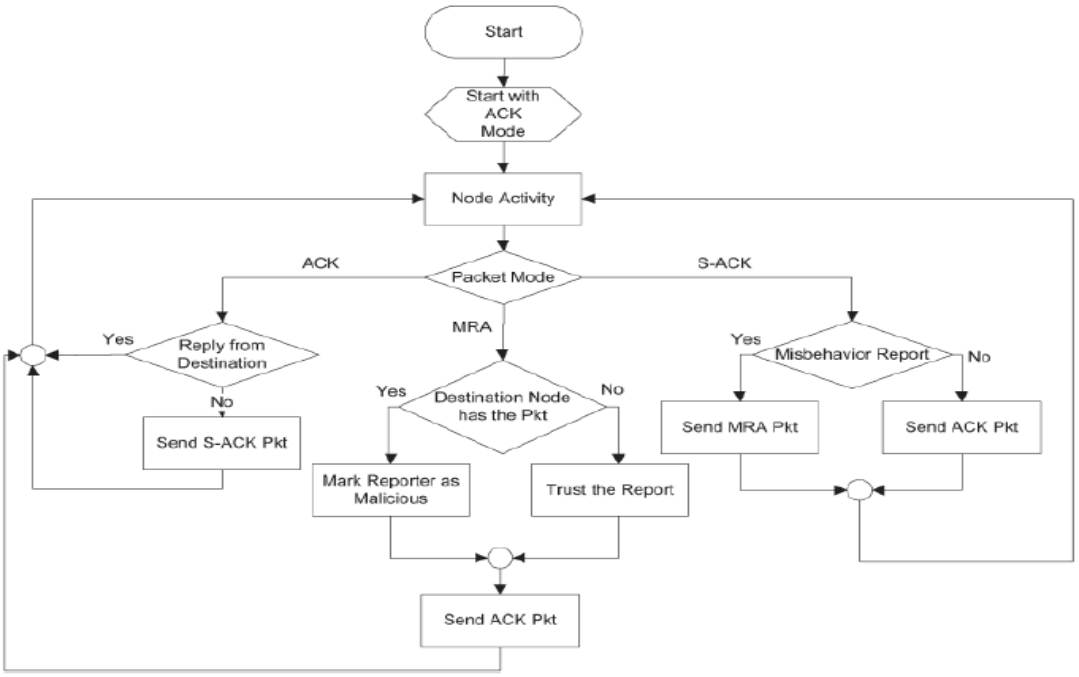

Fig. 4.2.1 S-ACK scheme: Node C is required to send back an acknowledgment packet to node A.

5. CONCLUSION AND FUTURE SCOPE

Packet-dropping attack has always been a major threat to the security in MANETs. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. To increase the merits of our research work, following issues to be investigated in our future research:

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 pre distributed keys;
3) Testing the performance of EAACK in real network environment instead of software simulation.

REFERENCES

[1] N.Soms, R.Saji Priya, A.S. Banu, P.Malathi, "A comprehensive performance analysis of zone based Intrusion Detection System in mobile ad hoc networks",IEEE Publisher, pp.1-8,26-28 March 2015.

[2] S.Adhikari, S.K. Setua, "Cooperative network intrusion detection system (CNIDS) in mobile adhoc network based on DSR protocol", IEEE Publisher, pp. 929 - 935, 12-13 Oct.2013.

[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] B.Kisku, R. Datta ,"An energy efficient scheduling scheme for Intrusion Detection System in Mobile Ad-hoc Networks", IEEE Publisher, pp.1-6, 6-8 Dec. 2012

[5] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgementsin MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis,Singapore, Mar. 22–25, 2011, pp. 488–494.

[6] 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

[7] 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

[8] 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., vol. 57, no. 3, pp. 813–819, Mar. 2010.

[9] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010

[10] 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.

[11] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind.Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[12] 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

[13] 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., vol. 55, no. 7,pp. 2759–2766, Jul. 2008

[14] 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

[15] 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.

[16] 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

[17] 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

[18] 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, pp. 191–199

[19] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in Proc. IEEE Int. Conf. Perform., Comput., Commun., 2004, pp. 747–752.

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

[21] 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

[22] 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

[23] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in Proc. Radio Wireless Conf., 2003, pp. 75–78

[24] 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

[25] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proc.ACM Workshop Wireless Secur., 2002, pp. 1–10

[26] 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

[27] 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

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

[29] 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.