Volume 4, Issue 8, August 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security in MANETs using EAACK

Parul Dubey
ME Scholar, G.S. Moze College of Engineering,
Pune, Maharashtra, India

Abstract —The migration to wireless network from wired network has become a global and emerging trend in the past few decades. The mobility and scalability are the features in wireless network which made it possible in many applications. Among all the contemporary wireless networks, Ad hoc Network (MANET) is one of the most and unique applications[1]. On the comparison with traditional network architecture, MANET does not require a fixed network infrastructure; every single node serves as a transmitter as well as a receiver. Nodes communicate directly with each other when both the transmitter and receiver are within the same communication range. Otherwise, they depend 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[1].On the other hand the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In such circumstances, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the improvements made in the field of technology and reducing the hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such a situation, we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement a intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to traditional approaches, EAACK demonstrates a higher malicious-behavior-detection rate in certain circumstances at the same time does not greatly affect the network performances.

Keywords—Digital signature, digital signature algorithm (DSA), Enhanced Adaptive ACKnowledgment (AACK) (EAACK), Ad hoc Network (MANET).

I. INTRODUCTION

Due to the natural mobility and scalability feature of wireless networks they are always preferred since the first day of their invention.With respect to the improvement in technology and objective of reducing costs, wireless networks have gained much more preferences over wired networks in the past few decades.

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.[1] Industrial remote access and control via wireless networks are becoming more and more popular these days [36]. The advantage of wireless networks which makes it unique is its ability to allow data communication between different parties and still maintain their mobility. However, this communication has a limitation that depends on the range of transmitters. This implies 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 taking the help of intermediate parties to relay data transmissions. This can be done by dividing MANET into two types of networks, namely, single-hop and multi hop. In a single-hop network, all nodes communicate directly with each other if they are within the same radio range. On the other hand, in a multi hop network, nodes depend on other intermediate nodes to transmit the data if the destination node is out of their radiorange. In comparison to the traditional wireless network, MANEThas a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [11], [28], [30]. MANET has the capability of creating a self-configuring and self-maintaining network that too 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 [20], [31].

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry [15],[29]. However, network security is very important considering the fact that MANET is popular among critical mission applications. Unfortunately, the cause like the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, malicious attackers can easily capture and compromise nodes to achieve attacks due to the nodes' lack of physical protection. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious [6], attackers can easily compromise MANETs by inserting malicious nodes into the network. Furthermore, a traditional centralized monitoring

technique is no longer feasible in MANET, the cause behind this is MANET's distributed architecture and changing topology. In such case, it is very essential to develop an intrusion-detection system (IDS) specially designed for MANETs. Many research efforts have been devoted to such research topic [1]–[4], [7]–[10], [16], [17], [23], [25], [27], [30]–[32].
In the next section, we will concentrate on discussing the background information required for understanding the concerned research topic.

II. BACKGROUND

A. 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 transmit data. This assumption allows the attackers giving them the opportunities to achieve significant impact on the network with just one or two compromised nodes. To solve this problem, IDS should be added in order to enhance the security level of MANETs. We will be able to completely eliminate the potential damages caused by compromised or alien nodes at the first time, If MANET can detect the attackers as soon as they enter the network,. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches [28]. Anantvalee and Wu [5] presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog [18], TWOACK [16], and Adaptive ACKnowledgment (AACK) [26].

1) Watchdog: the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog detects malicious misbehaviors by promiscuously being attentive to its next hop's transmission [37]. If a watchdog node overhears that its next node fails to forward the packet within a particular amount of given time, it will increase its failure counter. The Watchdog node reports a node as misbehaving when a node's failure counter exceeds a predefined threshold. Moreover, compared to another schemes, Watchdog is capable of police investigation malicious nodes instead of links [37]. The watchdog theme fails to observe malicious misbehaviors when it finds the presence of the following:
1) Ambiguous collisions
2) Receiver collisions
3) Restricted transmission power
4) False misbehavior report
5) Collusion
6) Partial dropping.

2) TWOACK: While considering the six weaknesses of the Watchdog theme, several researches projected new approaches to solve these problems. TWOACK detects misbehaving links by acknowledging each information packet transmitted over each three consecutive nodes on the trail from the supply to the destination [37]. TWOACK is needed to focus on routing protocols like Dynamic Supply Routing. The operating method of TWOACK can be viewed as Fig. 1: Node A primary forwards Packet 1 to node B, node B forwards Packet 1 to node C. Once node C receives Packet 1,because of the two hops from node A, node C will be duty-bound to come up with a TWOACK packet, that will contain a 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 one from node A to node C is successful. If this TWOACK packet is not received in a predefined period, each nodes B and C area unit report edmalicious. Identical methods are applied to each three consecutive nodes on the remainder of the route.

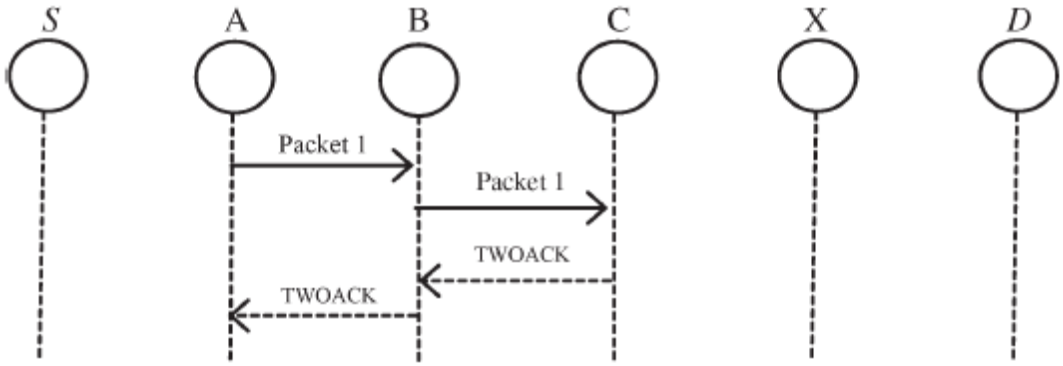

Fig.1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

3)AACK:This one is based on TWOACK and the newly proposed scheme is called as AACK. Almost like TWOACK, AACK is an Adaptive Acknowledgment-based network layer scheme which may be considered as the combination of a scheme called TWOACK associated an end-to-end acknowledgment scheme referred to as ACKnowledge[37]. AACK

considerably reduced network overhead at the same time it is still capable of maintaining surpassing identical network output. The end-to-end acknowledgment theme in ACK is given in Fig. 2. S is the supply node, sends outone with none overhead except two b of flag indicating the packet sort. All the intermediate nodes sequentially forward this packet. Once D, the destination node receives Packet one, it is needed to challenge associate ACK acknowledgment packet to the supply node S on the reverse order of identical route. Within a predefined period, if S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. ElseS can switch to TACK scheme by causation out a TACK packet. The conception of adopting a hybrid theme in AACK greatly reduces the network overhead, however each TWOACK and AACK still suffer from the matter that they fail to observe malicious nodes with the presence of false misbehaviors report and forged acknowledgment packets[37].

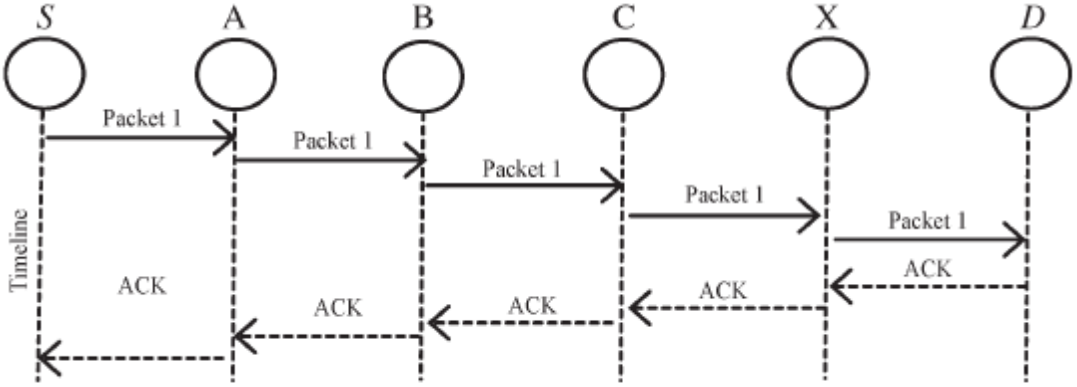

Fig.2. ACK scheme: The destination node is required to send acknowledgment packets to the source node.

B. Digital Signature

Digital Signature is a part of cryptography. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [37].

The MANET security is outlined as a mixture of processes, procedures, and systems used to ensured confidentiality, authentication, integrity, availability, and non repudiation. Digital signature is a widely adopted approach to confirm the authentication, integrity, and non repudiation of MANETs. To ensure the validity of the digital signature, the message is first sent to the hash function or in case the message is valid data means it directly send to the messages, and the hash function is processed and then it sends to the message digest, the message digest is used to check the validity of the message. After this it is sent to signature function, it checks signature is private key or public key.

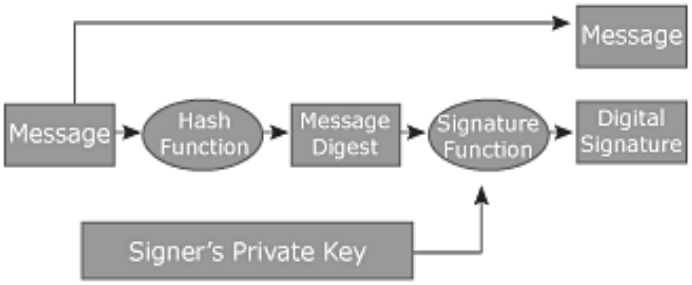

Fig.3. Communication with digital signature.

III. PROBLEM DEFINITION

Our proposed system EAACK is designed to tackle some of the weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. Here, we discuss these weaknesses in detail.

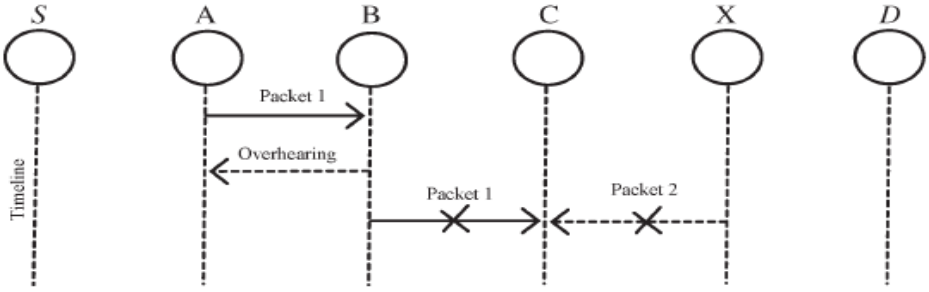

Fig.4. Receiver collisions: Both nodes B and X are trying to send Packet1 and Packet2, respectively, to node C at the same time.

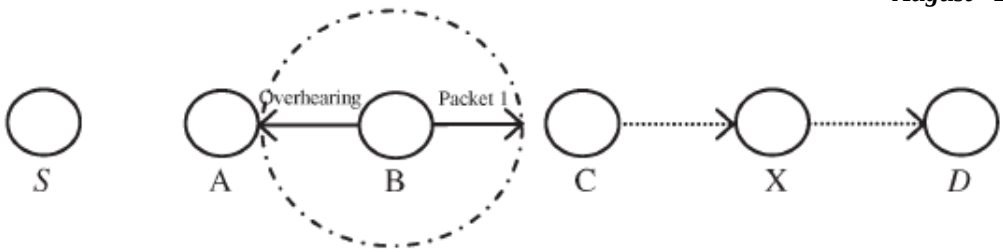

Fig.5. Limited transmission power: Node B limited transmission power so that the packet transmission can be over head by node A but too weak to reach node C.

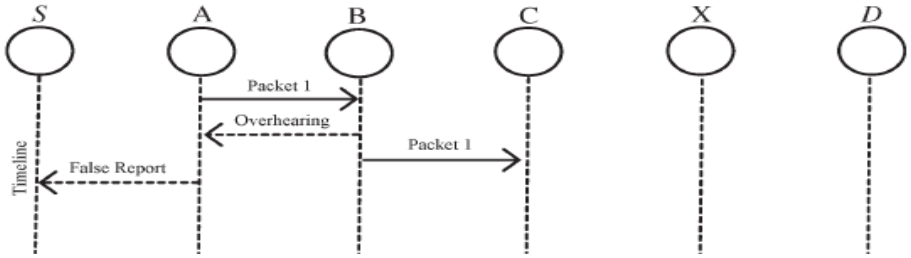

Fig. 6. False misbehavior report: Node A sends back a misbehavior reporteven though node B forwarded the packet to node C.

In an example of receiver collisions as shown in Fig. 4, once node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; in the meantime, node X is forwarding Packet 2 to node C. In this case, node A overhears that node B has successfully forwarded Packet 1 to node C however did not observe that C failed to receive this packet as a result of a collision between Packet 1 and Packet 2 at node C.

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

For false misbehavior 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[1]. Attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack, as a result of the open medium and remote distribution of typical MANETs.

IV. PROPOSED SYSTEM

EAACK is consisting of three major components, namely, ACK, secure ACK, and misbehavior report authentication. In order to distinguish different packet varieties in different schemes, we tend to enclose a 2-b packet header in EAACK[37].

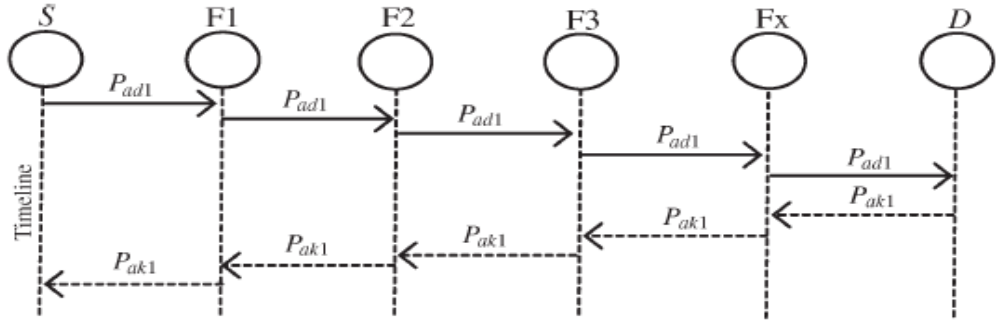

Fig.6.System controller flow: This figure show system flow the EAACK scheme works.

ACK

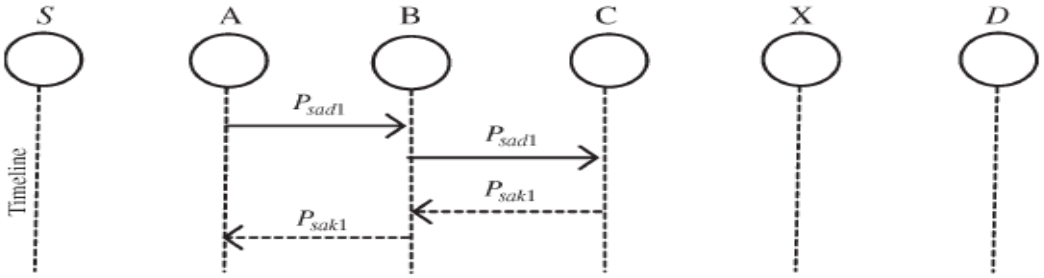

Fig. 8. ACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

ACK is basically an end-to-end acknowledgment scheme. When no network misbehavior is detected, it acts as a part of the hybrid scheme in EAACK with the aim to reduce network overhead. In Fig. 8, in ACK mode, node S initially 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[1]. Within a predefined time period, if S receives Pak1, then only the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode.

S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu et al. [16]. The motive here is to let every three consecutive nodes work in a group to detect misbehaving nodes. The third node is required to send an S-ACK acknowledgment packet to the first node, for every three consecutive nodes in route. Detection of misbehaving nodes in the presence of receiver collision or limited transmission power is the intention of introducing S-ACK mode. As shown in Fig. 9, 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 [1]. Firstly, node F1 sends out S-ACK data packet Psad1 to node F2. Secondly, node F2 forwards this packet to node F3. When node F3 receives Psad1, as F3 is the third node in this group, F3 is required to send back an S-ACK acknowledgment packet Psak1 to node F2. Node F2 forwards Psak1 back to node F1[1]. Both nodes F2 and F3 are pointed as malicious if node F1 does not receive this acknowledgment packet within a predefined time period. A misbehavior report will be generated by node F1 and will be sent to the source node S. Nevertheless, 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[1]. This is an important step to detect false misbehavior report in our proposed scheme.

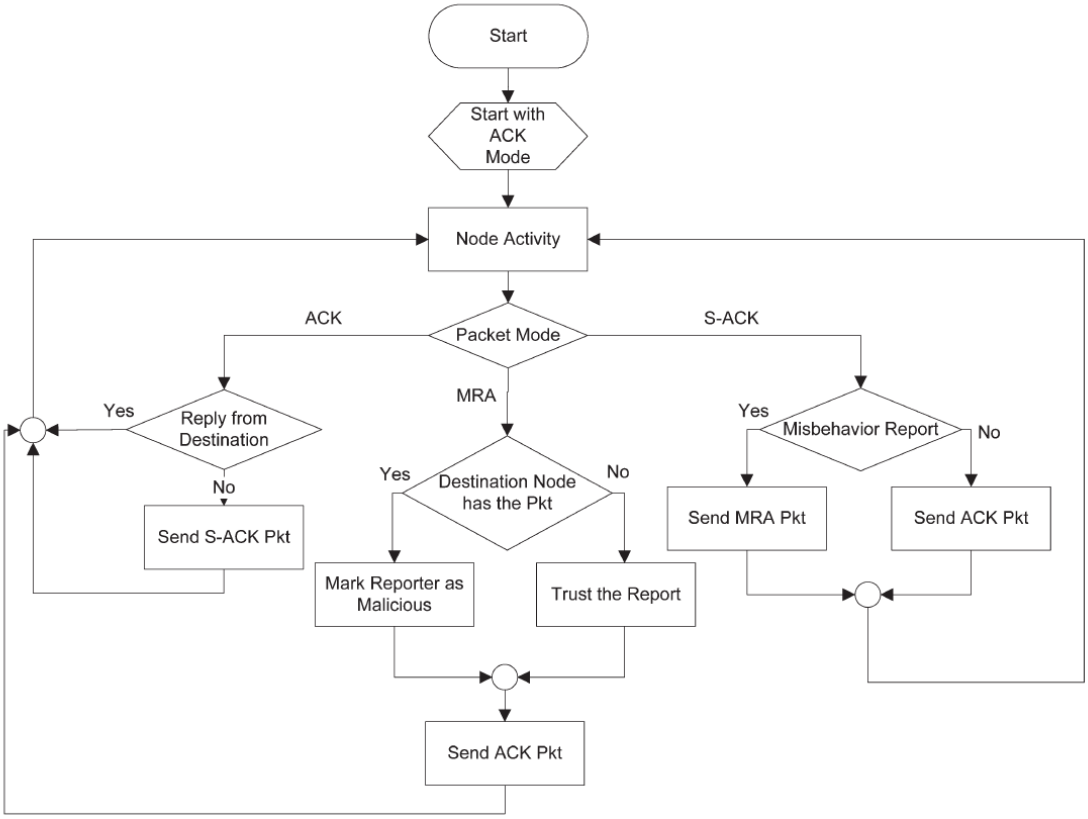

Fig. 9. S-ACK scheme: Node C is required to send back an acknowledgment packet to node A.

MRA

The MRA scheme is designed mainly to resolve the drawbacks of Watchdog when it fails to detect misbehaving nodes. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route [1]. To initiate the MRA mode, firstly, the source node searches its local knowledge base and seeks for an alternative route to the destination node. The source node starts a DSR routing request to find another route, if there is no other route exist. With the help of adopting an alternative route to the destination node, we circumvent the misbehavior reporter node. Similarly, when the destination node receives an MRA packet, it searches its local knowledge base and then compares if the reported packet was received already. If it is already received, then it can be concluded that this is a false misbehavior report. Meanwhile, whoever generated this report is marked as malicious. The misbehavior report is trusted and accepted in other conditions.

Digital Signature

All the components of EAACK, namely ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. All of them rely on acknowledgment packets to sight misbehaviors in the network. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable [1]. With reference to this, we tend to incorporated digital signature in our proposed scheme.

V. CONCLUSION

Packet-dropping is a major threat to the security in MANETs. In this research paper, we have proposed a IDS named EAACK protocol exclusively designed for MANETs. They can have positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Drawbacks of Watchdog is clearly mentioned. We conclude that this scheme is worthwhile when network security is the top priority.

REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami "EAACK—A Secure Intrusion- Detection System for MANETs" IEEE Trans on Industrial Electronics, vol. 60, no. 3, Mar 2013.

[2] 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.

[3] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc NetworkSecurity," in LectureNotes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[4] 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.

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

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

[7] 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.

[8] 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.

[9] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEEWorkshopMobile Comput. Syst. Appl., 2002, pp. 3-13.

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

[11] 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.

[12] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[13] 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.

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

[15] 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.

[16] 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.

[17] 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.

[18] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. MobileComput. Netw., Boston, MA, 2000, pp. 255–265.

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

[20] 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.

[21] 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.

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

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

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

[29] 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.

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

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

[32] L. Zhou and Z. Haas, "Securing ad-hoc networks," IEEE Netw., vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[33] Botan, A Friendly C ++ Crypto Library. [Online]. Available: http://botan.randombit.net/

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

[35] TIK WSN Research Group, The Sensor Network Museum—Tmote Sky.[Online]. Available: http://www.snm.ethz.ch/Projects/TmoteSky

[36] Y. Kim, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," IEEE Trans. Instrum.Meas., vol. 57,no. 7, pp. 1379–1387, Jul. 2008.

[37] K.Kirubani, S.P.Anbukodi, "A Secure Intrusion Detection System for Manets by using Cryptographic Algorithms" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol.3,Issue 3, Mar 2014.

