IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 2, April 2014.
www.ijiset.com
ISSN 2348 - 7968

Communicating Via Ant Colony Algorithm and Detecting Attackers through Tracking Program in MANETs

V.Ezhilarasi[#1], E. Vinothini [#2], K.Prabisha[#3], D. Nagamani Abirami[#4]

UG Student, Department Of Computer Science and Engineering[#1, 2, 3]
Assistant Professor, Department Of Computer Science and Engineering[#4]
Manakula Vinayagar Institute of Technology, Puducherry.

***Abstract* - In the past few decades migration from wired to wireless network has been a global trend. The most important and widely used application in wireless network is Mobile Ad-hoc Networks(MANETs). MANETs are considered to be the future wireless network consisting entirely of mobile nodes that communicate on-the-move without any base stations. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET. Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs is used for providing secure intrusion-detection system to protect MANET from attacks. As there is no efficiency in the existing system to find the attacker, in our proposed model we provide efficient communication path using Ant colony Algorithm which leaves duplicate messages throughout its travelling nodes like ants leaves pheromones for further ants to sense the path. Thus it helps us to sense the attacker and from which node the attack has taken place. A tracking program is sent along with the source to destination which waits for acknowledgement from the destination till it gets the acknowledgement. If it does not get acknowledgement it waits till acknowledgement and it resends to the destination. It helps finds out the attacker soon. We implies Elliptic Curve Cryptography (ECC) algorithm for ensuring security for the message to be sent along with acknowledgement.**

***Keywords*- Elliptic Curve Cryptography (ECC), Enhanced Adaptive ACKnowledgment(AACK)(EAACK), Mobile Ad hoc NETwork s(MANETs).**

I. INTRODUCTION

Due to their natural mobility and scalability, wireless networks are always preferred since the first day of their invention. Owing to the improved technology and reduced 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. Industrial remote access and control via wireless networks are becoming more and more popular these days [2]. 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 multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [10], [28]. 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 [19], [30].

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry [14],[28]. 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 promise 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 and presumably not malicious [5], 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 (IDS) specially designed for MANETs. Many research efforts have been devoted to such research topic [1]–[3], [6]–[9], [15], [16], [22], [24], [26].

ISSN 2348 - 7968

II. LITERATURE SURVEY

a. DoS Attacks in Mobile Ad Hoc Networks: A Survey

MANETs have unique characteristics like dynamic topology, wireless radio medium, limited resources and lack of centralized administration, as a result, they are vulnerable to different types of attacks in different layers of protocol stack. Each node in a MANET is capable of acting as a router. Routing is one of the aspects having various security concerns. In this paper we will present survey of common Denial-of-Service (DoS) attacks on network layer namely Wormhole attack, Black hole attack and Gray hole attack which are serious threats for MANETs[3]. We will also discuss some proposed solutions to detect and prevent these attacks. As MANETs are widely used in many vital applications, lots of research work has to be done to find efficient solutions against these DoS attacks that can work for different routing protocols.

b. Intrusion detection techniques in mobile ad hoc and wireless sensor networks

Mobile ad hoc networks and wireless sensor networks have promised a wide variety of applications. However, they are often deployed in potentially adverse or even hostile environments. Therefore, they cannot be readily deployed without first addressing security challenges. Intrusion detection systems provide a necessary layer of in-depth protection for wired networks. However, relatively little research has been performed about intrusion detection in the areas of mobile ad hoc networks and wireless sensor networks. In this article, first we briefly introduce mobile ad hoc networks and wireless sensor networks and their security concerns. In this paper we focus on their intrusion detection capabilities[4]. Specifically, we present the challenge of constructing intrusion detection systems for mobile ad hoc networks and wireless sensor networks, survey the existing intrusion detection techniques, and indicate important future research directions.

c. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks

An ad hoc network is a collection of wireless computers (nodes), communicating among themselves over possibly multihop paths, without the help of any infrastructure such as base stations or access points. Although many previous ad hoc network routing protocols have been based in part on distance vector approaches, they have generally assumed a trusted environment. In this paper,we design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol. In order to support use with nodes of limited CPU processing capability, and to guard against Denial of Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. SEAD performs well over the range of scenarios we tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.

d. Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks

An ad hoc network is a group of wireless mobile computers (or nodes), in which individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. Prior research in ad hoc networking has generally studied the routing problem in a non-adversarial setting, assuming a trusted environment. In this paper, we present attacks against routing in ad hoc networks, and we present the design and performance evaluation of a new secure on-demand ad hoc network routing protocol, called Ariadne[9]. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of Service attacks. In addition, Ariadne is efficient, using only highly efficient symmetric cryptographic primitives.

e. Detecting Forged Acknowledgements in MANETs

Over the past few years, with the trend of mobile computing, Mobile Ad hoc Network (MANET) has become one of the most important wireless communication mechanisms among all. Unlike traditional network, MANET does not have a fixed infrastructure, every single node in the network works as both a receiver and a transmitter. Nodes directly communicate with each other when they are both within their communication ranges. Otherwise, they rely on their neighbours to store and forward packets. As MANET does not require any fixed infrastructure and it is capable of self configuring, these unique characteristics made MANET ideal to be deployed in a remote or mission critical area like military use or remote exploration. However, the open medium and wide distribution of nodes in MANET leave it vulnerable to various means of attacks. It is crucial to develop suitable intrusion detection scheme to protect MANET from malicious attackers. In our previous research, we have proposed a mechanism called Enhanced Adaptive Acknowledgement (EAACK) scheme. Nevertheless, it suffers from the threat that it fails to detect misbehaving node when the attackers are smart enough to forge the acknowledgement packets. In this paper, we introduce Digital Signature Algorithm (DSA) into the EAACK scheme[13], and investigate the performance of DSA in MANETs.

ISSN 2348 - 7968

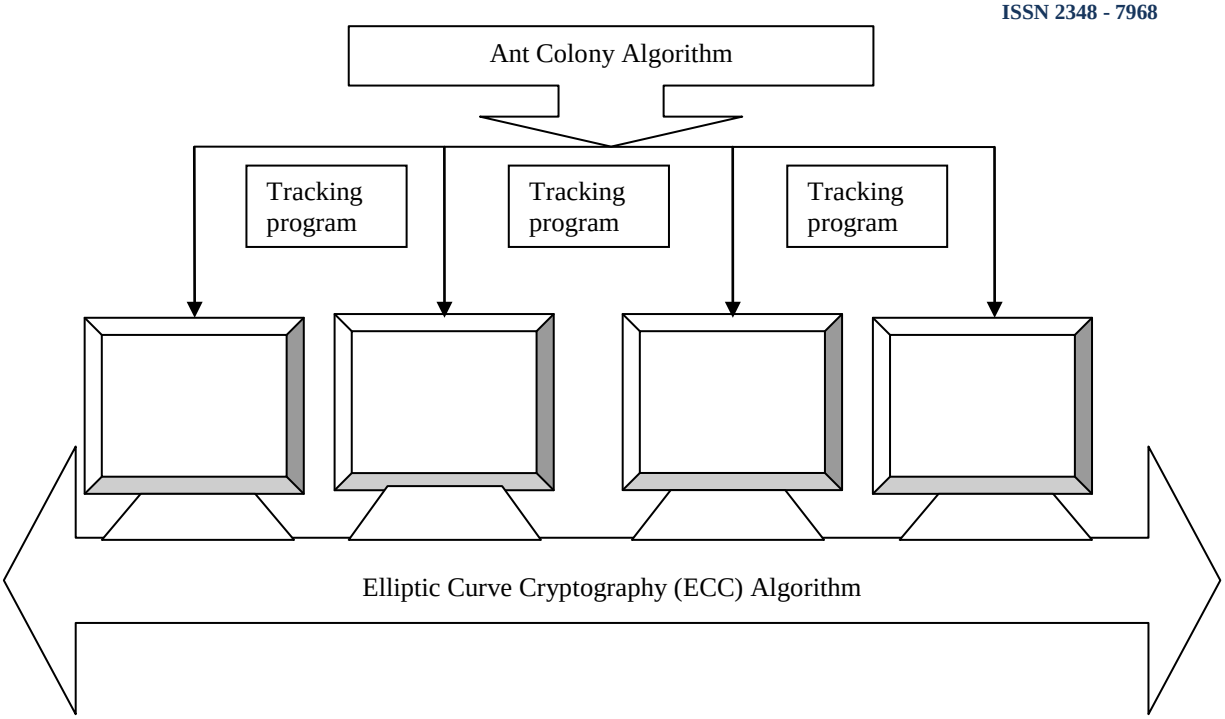

Fig. 1. System architecture

The purpose of this paper is to present an improved version of EAACK called EAACK2 that performs better in the presence of false misbehavior and partial dropping.

III. EXISTING SYSTEM

Mobile Ad hoc NETworks (MANETs) 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. Unfortunately, the open medium and remote distribution of MANETs make it vulnerable to various types of attacks.

There exists several intrusion detection system for detecting the attacks occurring. For secure intrusion detection system, digital signature is used.To adopt a digital signature Enhanced Adaptive ACKnowledgement (EAACK) scheme is used. EAACK is consisted of three major parts namely, ACK, S-ACK(secure-ACK), MRA(Misbehavior report authentication) here RSA and DSA scheme is used in implementation. Limitation of the existing system,

1) As there is no centralized system in MANETs it is difficult to identify the correct path in which the mobile nodes are moving.
2) Message authentication is checked for authorized users.
3) Forthcoming attacks have no prevention measures.

IV. PROPOSED SYSTEM

In our proposed model we provide efficient communication path using Ant colony Algorithm which leaves duplicate messages throughout its travelling nodes like ants leaves pheromones for further ants to sense the path. Thus it helps us to sense the attacker and from which node the attack has taken place. A tracking program is sent along with the source to destination which waits for acknowledgement from the destination till it gets the acknowledgement. If it does not get acknowledgement it waits till acknowledgement and it resends to the destination. It helps finds out the attacker soon. We implies Elliptic Curve Cryptography (ECC) algorithm for ensuring security for the message to be sent along with acknowledgement. Advantage of proposed system:

1) To find nodes communication path efficiently, we use Ant Colony Algorithm.
2) After the destination received the data, the acknowledgement is sent along with tracking program to the source, to identify the attackers attacking the acknowledgment.
3) To ensure security for sending messages we use Elliptic curve cryptography (ECC) algorithm.

V. MODULE DESCRIPTION

The proposed system of my project consists of following modules.

A. Server/Client Creation.

B. Implementing Ant Colony algorithm.

ISSN 2348 - 7968

C. Elliptic Curve Cryptography (ECC) Algorithm for ensuring security.
D. Tracking Program for Acknowledgement technique.

A. Server/Client Creation.

The server can maintain a database that update complete information about the client involved communication through the server. The server is created to support response to the client request so that server is in keep track of blocked ip address.

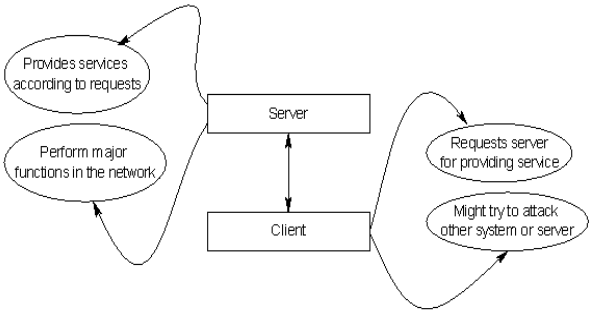

Fig. 2. Client/Server creation

B. Implementing Ant Colony algorithm

In ant colony algorithm, when ant searches for food source in a path, the other ants follows the path in which the previous ant is moving, it is because of the pheromone. The ants move until the food source is reached. When any obstacle occurs, it will choose another path, and moves towards food source. In similar way, in MANETs each node is considered as ant.

As the nodes are mobile, a node at source starts moving towards destination, other nodes follow the previous node path which leads to destination. Instead of pheromone, here the node leaves duplicate message, with the help of this other nodes follows it.

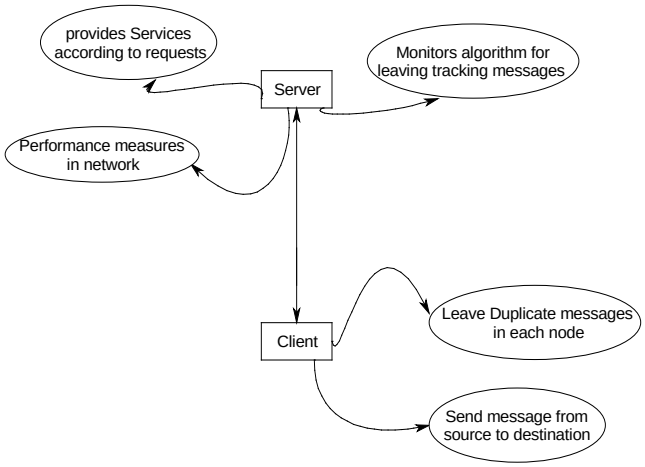

Fig. 3. Implementing Ant Colony algorithm

3) Elliptic Curve Cryptography (ECC) Algorithm for ensuring security.

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over fields Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization.

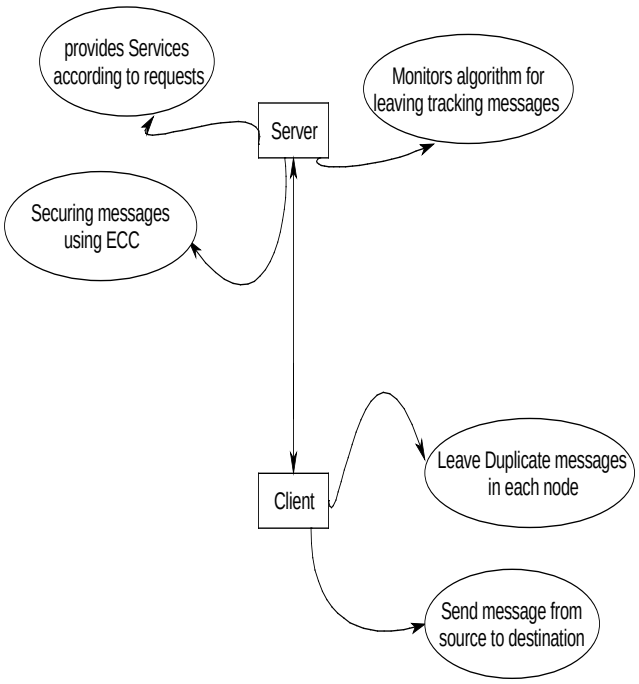

Fig. 4. ECC algorithm

4) Tracking Program for Acknowledgement technique.

When sender sends data to receiver, the receiver receives it and sends acknowledgment to the sender that data is received successfully.

When receiver does not send ACK or may be chance of missing ACK in between due to attackers. So sender will wait for particular time, and resends the data again. To overcome this, we should identify the attacker who is attacking the ACK.

Hence at the receiver side the ACK is sent along with tracking program which is a Java program.This program helps to identify from which IP address the attacker is attacking. As the nodes between the source and destination communicates in same IP address, if any change in IP address occurs, it is notified to the person who is managing the network.

ISSN 2348 - 7968

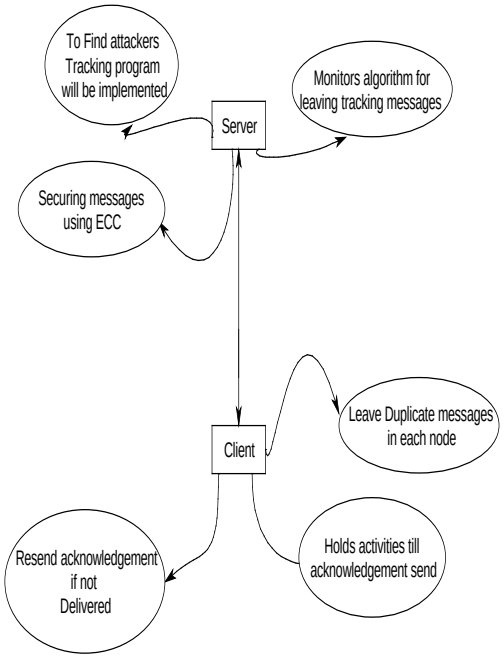

Fig. 5. Tracking program

V. PERFORMANCE EVALUATION

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].

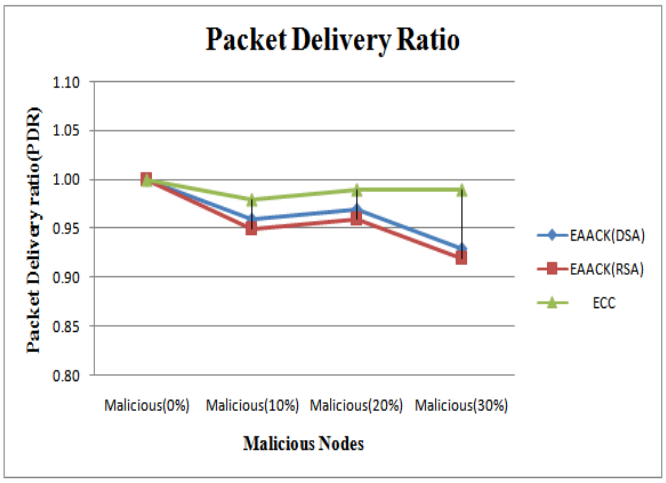

Fig. 6. Packet Delivery Ratio

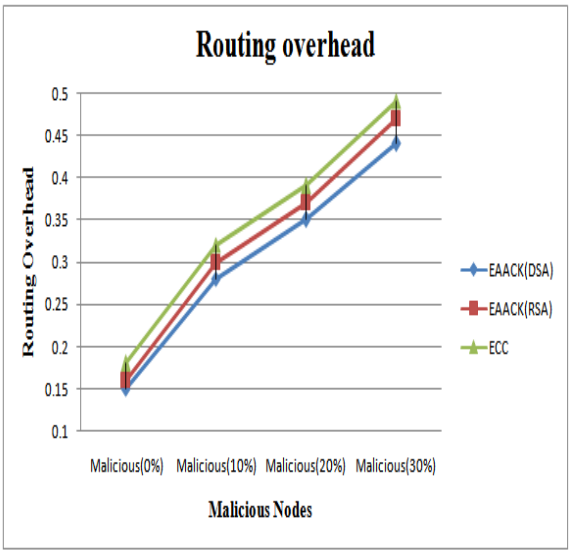

Fig. 7. Routing overhead

VI. CONCLUSION

Thus in our proposed model the secure communication is provided with the help of Elliptic Curve Cryptography (ECC). And also it is possible to find the attacker soon with the help of tracking program. Ant Colony algorithm is used to sense the attacker and from which node the attack has taken place.

VII. REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami "EAACK-A Secure Intrusion-Detection System for MANETs" *IEEE Trans. Ind. Electron.*, vol. 60, no. 3, pp. 1089–1098, Mar. 2013.

[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] 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.

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

[7] 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.

[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, pp. 3–13.

[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*, Atlanta, GA, 2002, pp. 12–23.

[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] 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.
[16] 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.
[17] 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.
[18] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996, T-37.
[19] 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.
[20] 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.
[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, pp. 75–78.
[22] 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.
[23] 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.
[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.*, vol. 57, no. 3, pp. 813–819, Mar. 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] 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.
[27] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.
[28] 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.