ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
Research Article
www.ijptonline.com

ENHANCED ADAPTIVE ACKNOWLEDGED SCHEME IN RECEIVER COLLISIONS

G. Charan reddy[1], M. SathishKumar[2]
UG Scholar, Assistance Professor, Saveetha School of Engineering, Saveetha University, Chennai.
Department of Computer Science, Saveetha School of Engineering, Saveetha University, Chennai.
Email: charanreddy7777@gmail.com

Received on: 18-05-2017 *Accepted on: 26-06-2017*

Abstract

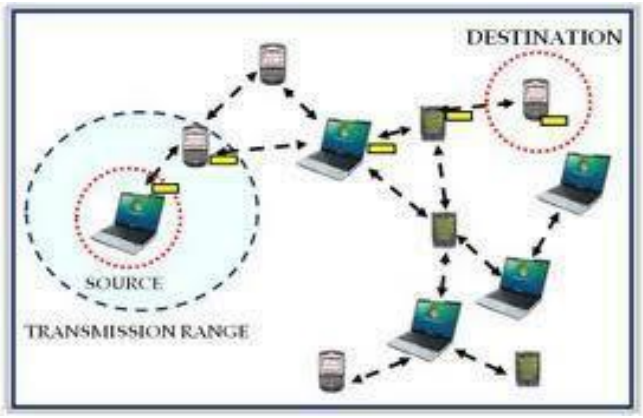
The migration to wireless network from wired network has been a world trend within the past few decades. The quality and quantifiability brought by wireless network created it doable in several applications. Among all the up to date wireless networks, Mobile spontanepous NET work (MANET) is one among the foremost necessary and distinctive applications. On the contrary to ancient specification, Edouard Manet doesn't need a set network infrastructure; each single node works as each a transmitter and a receiver. Nodes communicate directly with one another once they square measure each inside an equivalent communication vary. Otherwise, they place confidence in their neighbors to relay messages. The self-configuring ability of nodes inMANETmade it well-liked among important mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes create Edouard Manet prone to malicious attackers. during this case, it's crucial to develop economical intrusion-detection mechanisms to shield Edouard Manet from attacks. With the enhancements of the technology and cut in hardware prices, we tend to square measure witnessing a current trend of increasing MANETs into industrial applications. to regulate to such trend, we tend to powerfully believe that it's important to deal with its potential security problems. during this paper, we tend to propose and implement a brand new intrusion-detection system named increased adaptative Acknowledgment (EAACK) specially designed for MANETs. Compared to up to date approaches, EAACK demonstrates higher malicious-behavior-detection rates in bound circumstances whereas doesn't greatly have an effect on the network performances.

Introduction

The term Edouard Manet (Mobile impromptu Network) refers to a multihop packet primarily based wireless network composed of a group of mobile nodes that may communicate and move at an equivalent time, while not victimization

any quite fastened wired infrastructure. Edouard Manet is really self organizing and reconciling networks that may be shaped and distorted on-the-fly while not the necessity of any centralized administration. Otherwise, indicate "Mobile impromptu Network" A Edouard Manet may be a variety of impromptu network that may amendment locations and set up itself on the fly.

As a result of MANETS are mobile, they use wireless connections to attach to varied networks. This could be a customary Wi-Fi association, or another medium, like a cellular or satellite transmission.



The purpose of the painter social unit is to standardize IP routing protocol practicality appropriate for wireless routing application inside each static and dynamic topologies with augmented dynamics owing to node motion and different factors. Approaches ar supposed to be comparatively light-weight in nature, appropriate for multiple hardware and wireless environments, Associate in Nursingd address situations wherever MANETs ar deployed at the sides of an IP infrastructure. Hybrid mesh infrastructures (e.g., a mix of fastened and mobile routers) ought to even be supported by painterUsing mature parts from previous work on experimental reactive and proactive protocols, the WG can develop 2 Standards track routing protocol specifications:

Reactive painter Protocol (RMP)

Proactive MANET Protocol (PMP)

If vital commonality between RMRP and PMRP protocol modules is determined, the WG might attempt to keep company with a converged approach. Each IPv4 and IPv6 are going to be supported..The painter WG will develop a scoped forwarding protocol that may expeditiously flood knowledge packets to any or all taking part painter nodes. the first purpose of this mechanism may be a simplified best effort multicast forwarding operate. the employment of this protocol is meant to be applied solely inside painter routing areas and also the WG effort are going to be restricted to

routing layer style problems.The painter WG can pay attention to the OSPF-MANET protocol work inside the OSPF WG and IRTF work that's addressing analysis topics associated with painter environments.

Characteristics of MANET's:

In MANET, every node acts as each host and router. that's it's autonomous in behavior. Multi-hop radio relaying-once a supply node and destination node for a message is out of the radio vary, the MANETs ar capable of multi-hop routing. Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.

Types of MANET:

There are different types of MANETs including:

In VANETs – Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.

Vehicular ad hoc networks (VANETs) –Enables effective communication with another vehicle or helps to communicate with roadside equipments.

Internet Based Mobile Ad hoc Networks (iMANET) – helps to link fixed as well as mobile nodes.

Types of routing protocols in the MANET:

Two types of routing protocols:

Table-Driven Routing Protocols

Destination-Sequenced Distance-Vector Routing (DSDV)

Cluster head Gateway Switch Routing (CGSR) The Wireless Routing Protocol (WRP) Source-Initiated On-

Demand Routing Protocols

Ad-Hoc On-Demand Distance Vector Routing (AODV)

Dynamic Source Routing (DSR)

Temporally-Ordered Routing Algorithm (TORA)

Associativity-Based Routing (ABR)

Signal Stability Routing (SSR)

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a revolutionary change in the computing world: computing

will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society. In the ubiquitous computing environment, individual users utilize, at the same time, several electronic platform through which they can access all the required information whenever and wherever they may be. The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method: it is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous devices. The Mobile Ad Hoc Network is one of the wireless networks that have attracted most concentrations from many researchers.

A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following typical features:

Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants. Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes. Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc

environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

Vulnerabilities of the Mobile Ad Hoc Networks

Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. In this section, we discuss the various vulnerabilities that exist in the mobile ad hoc networks.

Lack of Secure Boundaries

The meaning of this vulnerability is self-evident: there is not such a clear secure *boundary* in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network.

In the wired network, adversaries must get physical access to the network medium, or even pass through several lines of defense such as firewall and gateway before they can perform malicious behavior to the targets. However, in the mobile ad hoc network, there is no need for an adversary to gain the physical access to visit the network: once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and thus join the network automatically. As a result, the mobile ad hoc network does not provide the so-called secure boundary to protect the network from some potentially dangerous network accesses.

Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can jeopardize the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks mainly include passive eavesdropping, active interfering, leakage of secret information, data tampering, message replay, message contamination, and denial of service.

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. 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. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations.Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or noncooperative 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.

Existing Methodology

Existing scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog schemeis consisted of two parts, namely, Watchdog and Pathrater. 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 Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

Proposed System

In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern, we adopt a digital signature in our proposed scheme named Enhanced AACK (EAACK). a new Intrusion-Detection system technique is used to prevent a malicious node in the MANETS, the malicious attacker used the wide distribution and open medium features of the MANETS to establish the vulnerabilities in the network. MANET is a self-configuring infrastructure network of mobile devices connected by wireless network it equipped with both a wireless transmitter and a receiver that communicate each other bidirectional wireless either directly or indirectly. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. 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. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks.

ACK implementation

ACK is basically an end – to – end acknowledgment scheme .It is a part of EAACK scheme aiming to reduce the network overhead when no network misbehavior is detected. The basic flow is if Node A sends an packet p1 to

destination Node D, if all the intermediate node are cooperative and successfully receives the request in the Node D. It will send an ACK to the source (Node A) , if ACK from the destination get delayed then it S-ACK process will be initialized.

Secure Acknowledgment (S-ACK)

In the S-ACK 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.

Security is a most significant challenge for generating a vigorous and consistent sensor networks, such as routing attacks have the capability to separate or isolate a sensor network from its Base Station (BS). Routing misbehavior in the network is that some malicious nodes will play in the route discovery and maintenance process but refuses to forward the data packets. In this project,I propose Secure Acknowledgement (S-ACK) based Routing Misbehavior Detection in Wireless Sensor Networks (WSN). Objective: The objective of this scheme is to identify the node misbehavior and reduce the overhead in WSN. Methods/Statistical Analysis: This scheme consists of 3 phase such as Acknowledgement (ACK) phase, Secure Acknowledgement (S-ACK) phase and (Misbehavior Verification) MV phase. If the source does not get the acknowledgement from the destination during ACK phase, the source sent the S-ACK packet to the S-ACK phase. S-ACK phase generates the misbehavior report. The Misbehavior Verification phase verifies the misbehavior.

Misbehavior Report Authentication (MRA)

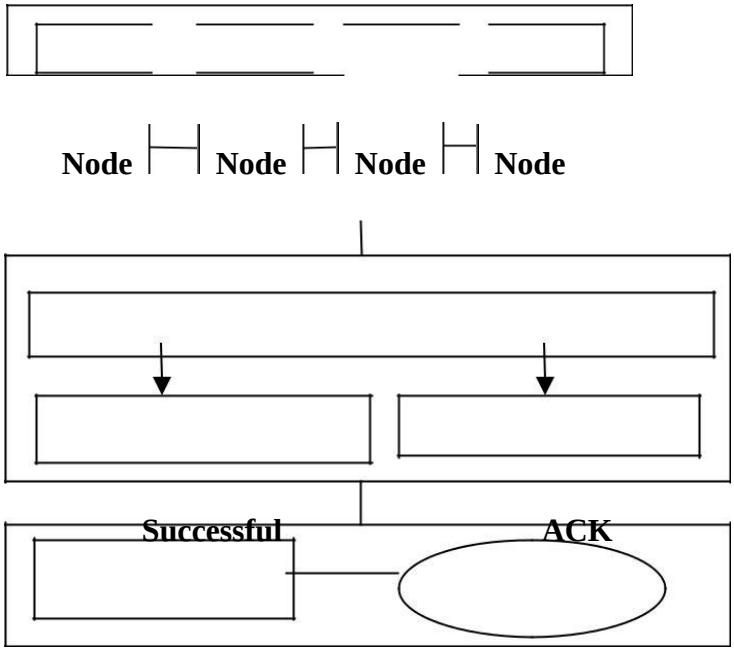
The MRA scheme is designed to resolve the weakness of watchdog with respect to the false misbehavior report. In this source node checks the alternate route to reach destination. Using the generated path if the packet reaches the destination then it is concluded as the false report.

When the packet reaches destination, FMR checks whether the packet is reached its destination or not through its local knowledge base. If there is any misbehavior node then it report to the source. When the watchdog detects a selfish node, it is marked as a positive detection (or a negative detection, if it is detected as a non-selfish node).MRA checks whether the packet is reached its destination or not through its local knowledge base. If destination has already received the same packet before, then MRA concludes that it is a false report and whichever node generated this report is marked selfish.

But if, the packet has reached its destination for the first time then the misbehavior report is trusted and accepted. Watch dog was intended for recognizing selfish node behavior in the network. In Watchdog next hop transmission is utilized for identifying selfish nodes.

Watch dog listens to its next hop transmission. On the off chance that a Watchdog hub catches that its next node neglects to forward the packet for a specific time period. Watch dog demonstrates the nearness of the childish hub to the source hub. The source node then broadcast the egotistical data to every single other node. At the point when the watch dog identifies a selfish node, it is set apart as a positive identification (or a negative recognition, on the off chance that it is recognized as a non-egotistical node).

Architecture diagram



SYSTEM IMPLEMENTATION

Development of three modules

It is a part of EAACK scheme aiming to reduce the network overhead when no network misbehavior is detected. The basic flow is if Node A sends an packet p1 to destination Node D, if all the intermediate node are cooperative and successfully receives the request in the Node D. It will send an ACK to the source (Node A) , if ACK from the destination get delayed then it S-ACK process will be initialized.

Security is a most significant challenge for generating a vigorous and consistent sensor networks, such as routing attacks have the capability to separate or isolate a sensor network from its Base Station (BS). Routing misbehavior in the network is that some malicious nodes will play in the route discovery and maintenance process but refuses to forward the data packets. In this project,I propose Secure Acknowledgement (S-ACK) based Routing Misbehavior Detection in Wireless Sensor Networks (WSN). Objective: The objective of this scheme is to identify the node misbehavior and reduce the overhead in WSN. Methods/Statistical Analysis: This scheme consists of 3 phase such as Acknowledgement (ACK) phase, Secure Acknowledgement (S-ACK) phase and (Misbehavior Verification) MV phase. If the source does not get the acknowledgement from the destination during ACK phase, the source sent the S-ACK packet to the S-ACK phase. S-ACK phase generates the misbehavior report. The Misbehavior Verification phase verifies the misbehavior.

MRA scheme is designed to resolve the weakness of watchdog with respect to the false misbehavior report. In this source node checks the alternate route to reach destination. Using the generated path if the packet reaches the destination then it is concluded as the false report. When the packet reaches destination, FMR checks whether the packet is reached its destination or not through its local knowledge base. If there is any misbehavior node then it report to the source. When the watchdog detects a selfish node, it is marked as a positive detection (or a negative detection, if it is detected as a non-selfish node).MRA checks whether the packet is reached its destination or not through its local knowledge base.

System Testing

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components,subassemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that theSoftware system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing

of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results.

An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

Conclusion

In this paper, I 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.

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. Elec-tron.*, vol. 56, no. 10, pp. 4266–4278, Oct. 2015.
2. R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Net-work Security," in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2015, 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, 2014, 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, 2013.
5. L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2013.
6. D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Model- ing 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. 2012.
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. 2012.
8. Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl.*, 2011, pp. 3–13.
9. Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand rout- ing protocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. MobiCom*, Atlanta, GA, 2011, pp. 12–23.
10. G. Jayakumar and G. Gopinath, "*Ad hoc* mobile wireless networks rout-ing protocol—A review," *J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582,2010.
11. D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 2010, ch. 5, pp. 153–181.

12. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. ii WAS*, Paris, France, Nov. 8–10,2009, pp. 216–222.
13. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowl- edgements in MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2008, pp. 488–494.
14. K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile *ad-hoc* commu- nications in AEC industry," *J. Inf. Technol. Const.*, vol. 9, pp. 313–323,2008.
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 misbe-haviour 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 misbe- haviour in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2007, pp. 255–265.