Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Mobile Wireless Intrusion Prevention System

Keerthi Sairam.D*
IT & Anna University
Tamil Nadu, India

Kaviya.T
ECE & Anna University
Tamil Nadu, India

Abstract: - The mobile ad hoc network is a new model of wireless communication and has gained increasing attention from industry. As in a general networking environment, mobile ad-hoc networks have to deal with various security threats. Due to its nature of dynamic network topology, routing in mobile ad-hoc network plays a vital role for the performance of the networks. It is understandable that most security threats target routing protocols – the weakest point of the mobile ad-hoc network. There are various studies and many researches in this field in an attempt to propose more secure protocols. However, there is not a complete routing protocol that can secure the operation of an entire network in every situation. Typically a secure protocol is only good at protecting the network against one specific type of attacks. Many researchers have been done to evaluate the performance of secure routing protocols in comparison with normal routing protocols. One of the objectives of this research is to examine the additional cost of adding a security feature into non-secure routing protocols in various scenarios. The additional cost includes delay in packet transmission, the low rate of data packets over the total packets sent, etc. It is well known that the real-world network does not operate in an ideal working environment, meaning that there are always threats and malicious actions affecting the performance of the network. Thus, studying the performance of secure routing protocols in malicious environments is needed in order to effectively evaluate the performance of those routing protocols. In the thesis, I have implemented two secure routing protocols: a secure version of the dynamic source routing - DSR and Secure Ad hoc on-demand Distance Vector routing protocol (SAODV) in the OPNET simulation environments. I will also create malicious scenarios by implementing several attacks in the simulation environments.

Keywords:- MANET, EAACK, IDS, AES, ECC

I. INTRODUCTION

A mobile ad hoc network 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. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc. Wireless networks have gained much more preferences over wired network for the past few decades owing to the improved technology and reduced costs. It is preferred to be the choice of most people since the day of invention due to their mobility and scalability. Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. In general, a wireless node can be any computing equipment that employs the air as the transmission medium.

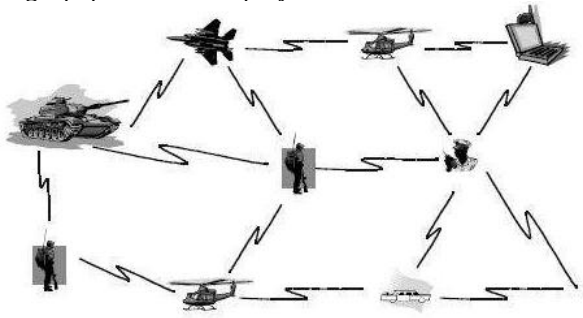

Fig. 1: Overview of Mobile Ad-hoc Network

As shown, the wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them. In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbour closer to the destination node. Due to the nature of an ad - hoc network, wireless nodes tend to keep moving rather than stay still. Therefore the network topology changes from time to time.

II. BACKGROUND

A.IDS AND MANETs

IDSs on MANETs use a variety of intrusion detection system. The most commonly proposed intrusion detection method to date is specification based detection. This can detect attacks against routing protocols with a low rate of false positives. Unfortunately, mobility of MANETs increases the rate of false positives in these systems. There have been few signatures based IDSs developed for MANETs and a little research on signature of attacks against MANETs. Since nodes in MANETs have only local data, a distributed and cooperative IDS architecture is generally used to provide a more informed detection approach. In this section, we mainly describe about EAACK an existing approach.

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different sc hemes to include a 2-b packet header in EAACK. According to the Internet draft of DSR, there is 6 b reserved in the DSR header. In EAACK, use 2 b of the 6 b to flag different types of packets.

DATA	ACK	S-ACK	MRA

Fig. 2: EAACK protocol in MANETs

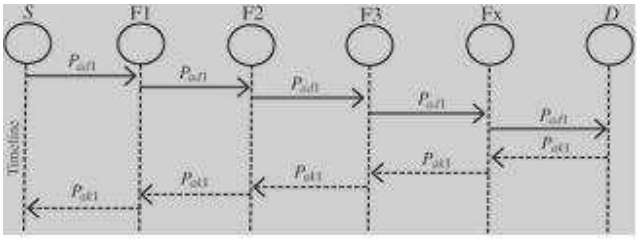

Fig. 3: System control flow of EAACK

In these secure IDS, It is assumed that the link between each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious. All acknowledgment packets are required to be digitally signed by its sender and verified by its receiver.

1) ACK: ACK is basically an end-to-end ACK IDS.[9][5] It acts as a part of the hybrid IDS in EAACK, aiming to reduce network overhead when no network misbehaviour is detected. Consider the scenario source node first sends out an ACK data packet to the destination node D. If all the intermediate nodes along the route between nodes S and Dare cooperative and node D successfully receives packet, node D is required to send back an ACK acknowledgment packet along the same route but in a reverse order. Within a predefined time period, if node S receives packet, 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.
2) S-ACK: It is an improved version of the TWOACK IDS. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.
3) MRA: Unlike the TWOACK IDS, where the source node immediately trusts the misbehaviour report, EAACK requires the source node to switch to MRA mode and confirm this misbehaviour report. This is a vital step to detect false misbehaviour. The MRA field is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour. The false misbehaviour report can be generated by malicious attackers to falsely report innocent nodes as malicious. The core of MRA field 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.
4) 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 misbehaviour report and whoever generated this report is marked as malicious. Otherwise, the misbehaviour report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehaviour report.

Packet Type	Packet Flag
General Data	00
ACK	01
S-ACK	10
MRA	11

Fig. 4: Packet type indicators

5) Digital Signature: EAACK is an acknowledgment-based ID. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on ACK packets to detect misbehaviours in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. To overcome this problem, need to incorporate digital signature in secure IDS.

B. Watch Dog

The main aim of watchdog is to increase the throughput of the network with the presence of malicious notes. The watchdog scheme consist of two parts namely watchdog and path rater. Watchdogs serve as IDS for MANETs. It is responsible for detecting the malicious node misbehaviors in the network. Watchdog detects malicious misbehavior by promiscuously listening to its next hop‘s transmission. If a watchdog node overhears that it_s next node fails to forward the packet within a certain period of time it increases its failure counter. Whenever a node failure counter exceeds predefined threshold, the watch dog node reports it as misbehaving in this case the path rater co-operates with the routing protocols to avoid the repeated nodes in future transmission.[14] Many following research studies and implementation have proved that the watchdog scheme is efficient. Furthermore, compared to some other schemes, watchdog is capable of detecting malicious nodes rather than links.[10] These advantages have made the watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as improvement to the watchdog scheme. The watch dog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collision; 2) receiver collision; 3) limited transmission power; 4) false misbehavior report; 5) collision; and 6) partial dropping.

III. PROBLEM DESCRIPTION

In the previous paper EAACK was an acknowledgement based scheme, where a digital signature is introduced for preventing the attacker from forging the acknowledgement packets. Since an additional scheme is introduced here for protecting the acknowledgement higher bandwidth is optimized. The EAACK scheme uses two algorithms DSA and RSA in which the key size is larger and process is longer here we tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. In this section, finally, complete content and organizational editing before formatting.[16] Please take note of the following items when proofreading spelling and grammar:

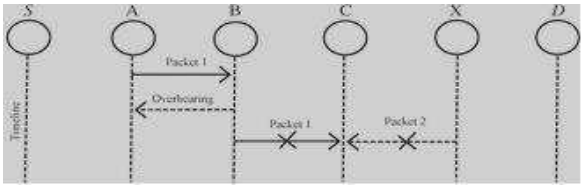

Fig. 5. Receiver collisions

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

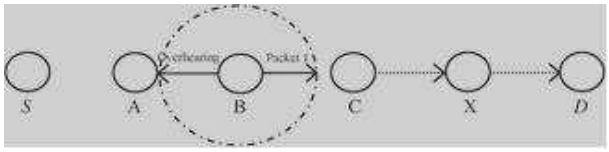

Fig. 6. Limited transmission power

Node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

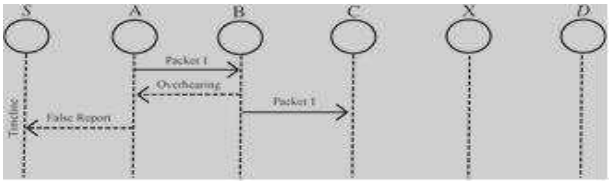

Fig. 7. False misbehavior report

Node A sends back a misbehavior report even though node B forwarded the packet to node C. In a typical example of receiver collisions, , after node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, node A overhears that node B has successfully forwarded Packet 1 to node C but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C. In the case of limited transmission power, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong 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. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack. As discussed in previous sections, 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 this research work, 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. Furthermore, we extend our research to adopt a digital signature scheme during the packet transmission process. As in all acknowledgment-based IDSs, it is vital to ensure the integrity and authenticity of all acknowledgment packets.

IV. SCHEME DESCRIPTION

In this section, we describe our proposed HYBRID CRYPTOGRAPHY TECHNIQUES in detail. The approach described in this research paper is based on the previous work of DSA and RSA algorithms where the key size is larger and requires a large storage space and higher transmission power. Here the scheme describes about two algorithms AES (Advanced Encryption Standard) and ECC (Elliptic Curve Cryptography) with the help of these algorithms the problems of the previous scheme are eliminated. Please note that, in our proposed scheme we assume that the link between each node in the network is bidirectional. Furthermore, for each communication process both the source node and destination node are not malicious

A.AES

AES is based on a design principle known as a substitution-permutation network, and is fast in both
software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block_size of 128bits, and a key_ size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4×4 column major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, and called the cipher text. Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

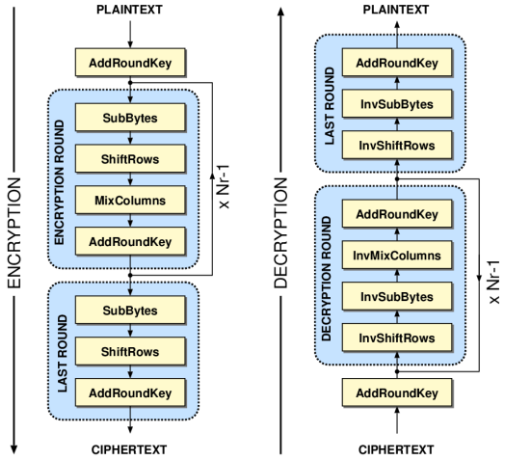

Fig. 8: process of AES

B. ECC(Elliptic curve cryptography)

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization. For elliptic-curve- based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible — this is the "elliptic curve discrete logarithm problem" or ECDLP. The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the difficulty of the problem.

The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key – e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key

V. PERFORMANCE ANALYSIS

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

A. Simulation Methodologies

To better investigate the performance of HYBRID CRYPTOGRAPHY under different types of attacks,
We propose three scenario settings to simulate different types of misbehaviors or attacks.

Scenario 1: In this scenario, we simulated a basic packet-dropping attack. Malicious nodes simply drop all the packets that they receive. The purpose of this scenario is to test the performance of IDSs against two weaknesses of Watchdog, namely, receiver collision and limited transmission power.

Scenario 2: This scenario is designed to test IDSs'performances against false misbehavior report. In this case, malicious nodes always drop the packets that they receive and send back a false misbehavior report whenever it is possible.

Scenario 3: This scenario is used to test the IDSs'performances when the attackers are smart enough to forge acknowledgment packets and claiming positive result while, in fact, it is negative. As Watchdog is not an acknowledgment-based scheme, it is not eligible for this scenario setting.

B. Simulation Configuration

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Ubuntu 9.10. The system is running on a laptop with Core 2 Duo T7250 CPU and 3-GB RAM. In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS 2.34. The intention is to provide more general results and make it easier for us to compare the results. In NS 2.34, the default configuration specifies 50 nodes in a flat space with a size of 670 × 670 m. The maximum hops allowed in this configuration setting are four. Both the physical layer and the 802.11 MAC layer are included in the wireless extension of NS2. The moving speed of mobile node is limited to 20 m/s and a pause time of 1000 s. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of
512 B. For each scheme, we ran every network scenario three times and calculated the average performance.

C. Simulation Results

Various scenarios are analysed and simulated through the graph for HYBRID CRYPTOGRAPHY and EAACK. These results show the proposed system shows a better performance than all the previous process and avoids several disadvantage of EAACK.

Scenario 1: The first scenario deals with the packet delivery ratio. Our proposed scheme HYBRID CRYPTOGRAPHY surpassed EAACK performance by 21%when there are 20% of malicious nodes in the network. From the results, we conclude that acknowledgment-based schemes, including TWOACK, AACK, and EAACK, are able to detect misbehaviours with the presence of receiver collision and limited transmission power. However, when the number of malicious nodes reaches 40%, our proposed scheme HYBRID CRYPTOGRAPHY performance is lower than those of TWOACK and AACK. We generalize it as a result of the introduction of MRA scheme, when it takes too long to receive an MRA acknowledgment from the destination node that the waiting time exceeds the predefined threshold.The simulation results of RO observe that AES and ECC scheme achieve the best performance, as they do not require acknowledgment scheme to detect misbehaviors. For the rest of the IDSs, AACK has the lowest overhead. This is largely due to its hybrid architecture, which significantly reduces network overhead. Although EAACK requires digital signature at all acknowledgment process, it still manages to maintain lower network overhead in most cases. We conclude that this happens as a result of the introduction of our hybrid scheme.

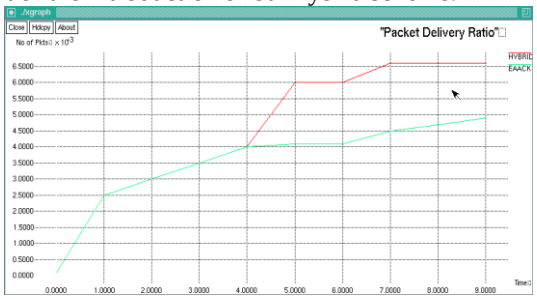

Fig. 9: Packet delivery ratio

Scenario 2: In scenario 2, we provide an average end to end delay and show how does a delivery of the packet get delayed while transmission. The HYBRID CRYPTOGRAPHY technique shows a better performance of packet delay when compared with EAACK

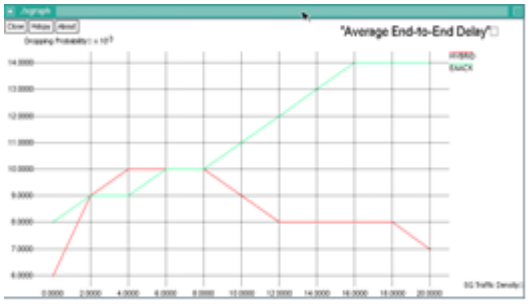

Fig. 10: Average end to end delay

Scenario 3: In scenario 3 , we provide information about the throughput ratio i.e the successful rate of packet delivery with our proposed system we get a better performance with the other schemes. There is 8% higher throughput ratio in the network with the presence of 20% malicious nodes, when the nodes get decreased the ratio increases and when it get higher it remains the same.

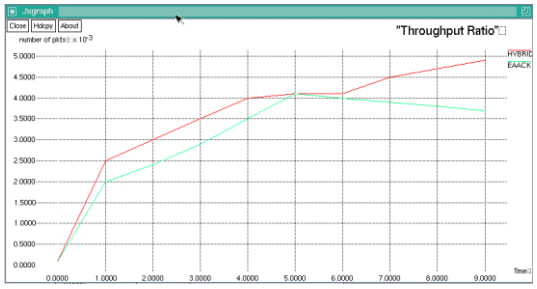

Fig. 11: Throughput ratio

VI. CONCLUSION AND FUTURE WORK

Packet dropping attack has been a major threat to the security in MANETs. In this research paper, we have proposed a new technique called HYBRID CRYPTOGRAPHY and compared it with the other scheme called EAACK in different scenarios through simulation. The results demonstrated a positive performance against EAACK in various scenarios such as throughput ratio, average end to end delay and packet delivery ratio. The process of this technique evaluated a faster process with less storage space and transmission power with the other scheme and algorithms.

To increase the merits of this research work, we plan to investigate the following issues in future

1. Possibilities of adopting a technique by which each and every node entry and exit requires a authentication process for enhanced security in network.
2. Try new techniques or algorithms so that the process might be faster with an enhanced performance.
3. Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre-distributed key.
4. Testing the performance of HYBRID CRYPTOGRAPHY TECHNIQUE in real network environment instead of software simulation.

REFERENCES

[1] 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, 2012, pp. 659–666.

[2] 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.

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

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

[5] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, ―Model-ing and optimization of a solar energy harvester system for self-powered

[6] wireless sensor networks,‖ IEEE Trans. Ind. Electron., vol. 55, no. 7, 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 IEEE Workshop Mobile Comput. Syst. Appl., 2002, 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, 2002, 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, 2007.

[11] D. Johnson and D. Maltz, ―Dynamic Source Routing in ad hoc wireless networks,‖ in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, 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,

[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, 2011, 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, 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, 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, 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 dis-covering 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.

