IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013
ISSN: 2320 - 8791
www.ijreat.org

An Enhanced Secure Detection And Analysis Of Bit Error Rate For Wireless Sensor Networks

B.Naghadevi[1], N.Nagaraj[2], V.Yokesh[3]

[1,2,3] ELECTRONICS AND COMMUNICATION ENGINEERING, ANNAUNIVERSITY/
PRATHYUSHA INSTITUTE OF TECHNOLOGY AND MANAGEMENT/THIRUVALLUR

Abstract: **Wireless Sensor Network(WSN) is one of the most important and unique applications. On the contrary to traditional network architecture, WSN does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbours to relay messages. The self-configuring ability of nodes in WSN made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make WSN vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect WSN from attacks.**

With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding WSN into industrial applications. To adjust to such trend, we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for WSN. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances. In EAACK scheme the wireless sensor network is going to be analysed in terms of Bit error rate (BER).

Keywords— Enhanced Adaptive ACKnowledgment ((EAACK), Wireless. Sensor Network(WSN),Intrusion Detection System (IDS), Misbehavior Report Authentication (MRA).

I. INTRODUCTION

A wireless sensor network is a collection of nodes organized into a cooperative network . Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single omni-directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated. Such systems can revolutionize the way we live and work.

Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the Internet. This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental,medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces.

Since a wireless sensor network is a distributed real-time system a natural question is how many solutions from distributed and real-time systems can be used in these new systems? Unfortunately, very little prior work can be applied and new solutions are necessary in all areas of the system. The main reason is that the set of assumptions underlying previous work has changed dramatically.

Most past distributed systems research has assumed that the systems are wired, have unlimited power, are not real-time, have user interfaces such as screens and mice, have a fixed set of resources, treat each node in the system as very important and are location independent. In contrast, for wireless sensor networks, the systems are wireless, have scarce power, are real-time, utilize sensors and actuators as interfaces, have dynamically changing sets of resources aggregate behavior is important and location is critical. Many wireless sensor networks also utilize minimal capacity devices which places a further strain on the ability to use past solutions.

Owing to these unique characteristics, WSN is becoming more and more widely implemented in the industry [14], [28]. However, considering the fact that WSN is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of WSN 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 WSNs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious [5], attackers can easily compromise WSNs by inserting malicious or non cooperative nodes into the network. Furthermore, because of WSN's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in WSNs.

In such case, it is crucial to develop an intrusion-detection system (IDS).

II. BACKROUND

In this paper we going to consider three different approaches as a backround information they are as follows:

1. IDS systems for wireless sensor networks.
2. Previous approach.
3. EAACK scheme.

III. ELLABORATION

1.*IDS systems for wireless sensor networks:*

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. An issue too often overlooked when considering intrusion detection is management - securely managing the system itself. Embraced within this aspect is reporting... it is essential that the reporting and analysis tools are first class, enabling proper interpretation of detected events. Within the Dragon IDS suite the Dragon Server component facilitates secure management of all Dragon Sensors and Dragon Squires. It also aggregates all alerts into one central database so that disparate attack information can be correlated.

network-based vs. host-based systems: in a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall simplistic filtering rules. In a host-based system, the IDS examines at the activity on each individual computer or host.

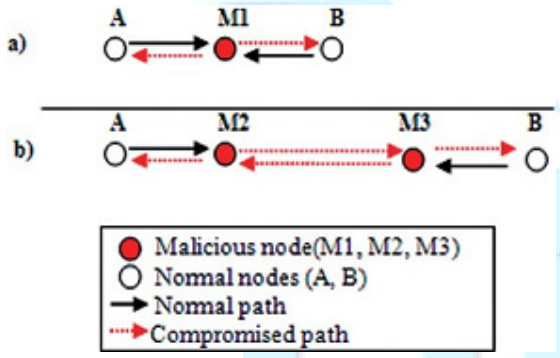


Figure 1. malicious node detection

In the above figure 1.the node A and B have to communicate between them in a normal path .but the node M1 ,M2,M3 are the malicious node which alter the path of A and B .These malicious nodes are called as intruding nodes and detection of this nodes is called as intrusion detection

2. Previous approach.:

In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK , and Adaptive ACKnowledgment (AACK).

1.Watchdog:

Watchdog to detect the misbehaving nodes.Watchdog aims to improve throughput of network with the presence of malicious nodes. In fact, the watchdog scheme is consisted of two parts, namely Watchdog and Pathrater. Watchdog serves as an intrusion detection system for WSN. It is responsible for detecting malicious nodes misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If 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. Many following researches and implementations have proved that the Watchdog scheme to be efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made Watchdog scheme a popular choice in the field. Many WSN IDSs are either based on or developed as an improvement to the Watchdog scheme.

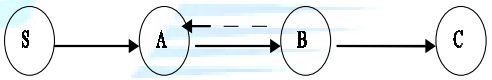


Fig 2.Operation of the watchdog.

Figure 2.illustrates the operation of the watchdog. Node A cannot transmit all the way to node C, but it can listen to node B's traffic. Thus, when A transmits a packet for B to forward to C, A can often tell if B transmits the packet. If encryption is not performed separately for each link, which can be expensive, then A can also tell if B has tampered with the payload or the headers. We implement the watchdog by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If the packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node

Limitations of Watchdog:

The watchdog mechanism can detect misbehaving nodes at forwarding level and not at the link level. Watchdog scheme fails to detect malicious misbehaviors with the presence of

- ambiguous collisions,
- receiver collisions,
- limited transmission power,
- false misbehavior report,
- partial dropping.
- collusion

2.TWOACK:

TWOACK is neither an enhancement nor a Watchdog based scheme. With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu *et al.* [16] is one of the most important approaches among them.

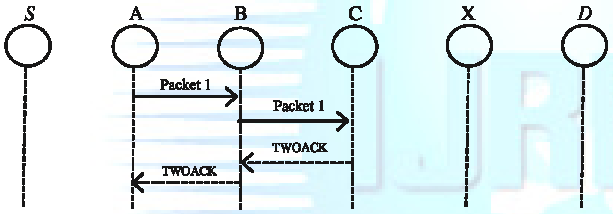


Fig.3. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

On the contrary to many other schemes,Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR). The working process of TWOACK is demonstrated in Fig. 3. node A first forwards packet 1 to node B, and then node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains 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 the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgement process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of WSN, such redundant transmission process can easily degrade the life span of the entire network.

3.AACK:

Based on TWOACK, proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

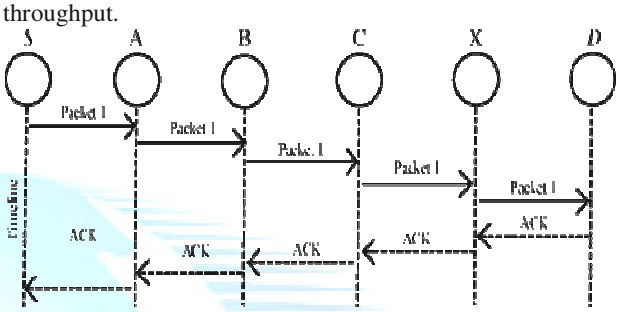


Fig.4 ACK scheme: The destination node is required to send acknowledgment packets to the source node.

In the ACK scheme shown in Fig. 4, the source node S sends out Packet 1 without any overhead except 2 b of flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

DRAWBACK OF ABOVE APPROACHES:

1. Receiver collision

In the receiver collision problem as illustrated in the figure 5.the node A can only identify whether node B has sent the packet to node C, but node A cannot assure that node C has received it. If a collision occurs at node C when node B first forwards the packet, node A can only assume that node B has forwarded the packet and assumes that node C has successfully received it. Thus, B could skip retransmitting the packet and evade detection.

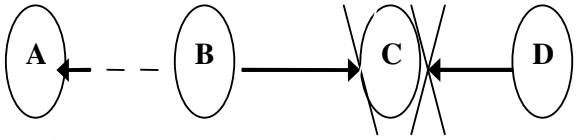


Fig 5 Receiver Collision.

2.Limited transmission power:

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. 6 below

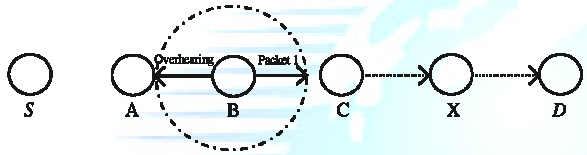


Fig. 6. Limited transmission power: Node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

3.**False misbehaviour report:**

For false misbehavior report, although node A successfully overheard that node B forwarded Packet 1 to node C, node Astill reported node B as misbehaving, as shown in Fig. 7. Due to the open medium and remote distribution of typical WSNs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack

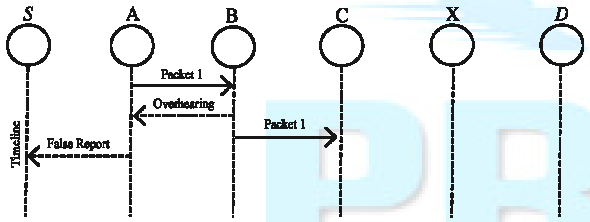


Fig. 7.False misbehavior report: Node A sends back a misbehavior report even though node B forwarded the packet to node C.

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 a new IDS specially designed for WSNs, which solves not only receiver collision and limited transmission power but also the false misbehavior problem.

3.EAACK SCHEME:

In this section, we describe our proposed EAACK scheme in detail. The approach described in this research paper is based on our previous work [12], where the backbone of EAACK was proposed and evaluated through implementation. In this paper, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgment packets.

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).

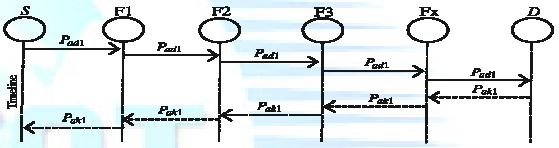


Fig. 8 System control flow: This figure shows the system flow of how the EAACK scheme works.

Fig. 8 presents a flowchart describing the EAACK scheme. 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 the destination node are not malicious. Unless specified, all acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver.

ACK:

ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In ACK mode, in figure 9 node S first sends out an ACK data packet ad1 P to the destination node D. If all the intermediate nodes along the route between node S and node D are cooperative and node D successfully receives ad1 P, node D is required to send back an ACK acknowledgement packet ak1 P along the same route but in a reverse order. Within a predefined time period, if node S receives ak1 P, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

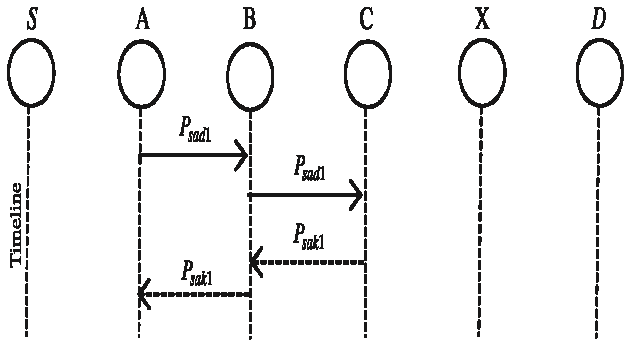


Fig. 9. ACK scheme

S-ACK:

The S-ACK scheme is an improved version of the TWOACK scheme 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.

MRA :

The Misbehavior Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. False misbehavior report can be generated by malicious attackers to falsely report that innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division.

The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is none other exists, the source node starts a DSR routing request to find another route. Due to the nature of WSNs, it is common to find out multiple routes between two nodes.

By adopting an alternative route to the destination node, we circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received, then it is safe to conclude this is a false misbehavior report and whoever generated this report is marked as malicious.Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

IV. PERFORMANCE OF EACH APPROACHES

1.IDS system of WSN:

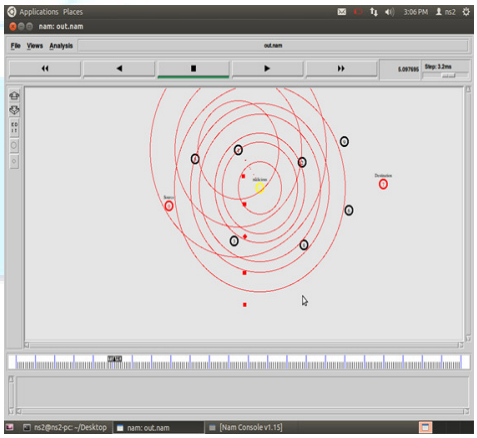
In a network some nodes can be selfish and malicious which leads to security concerns. Therefore, Intrusion Detection System (IDS) is required for WSN. In WSN, most of the Intrusion Detection Systems (IDSs) are based on watchdog technique. These watchdog techniques also called overhearing techniques and suffer from some problems. In this paper an effort has been made to overcome the problems of overhearing technique. Intrusion Detection Systems (IDSs) for (WSN) are indispensable since traditional intrusion prevention based techniques are not strong enough to protect WSN. However, the dynamic environment of WSN makes the design and implementation of IDSs. Wireless ad-hoc networks need to be secured and use intrusion detection systems (IDS).

The initial phase of project is IDS system.In IDS 10 nodes are assumed to be placed in the network simulator .Make any one node to be a malicious node and allow the data to be passed through it. We can visually see the data loss between each node.

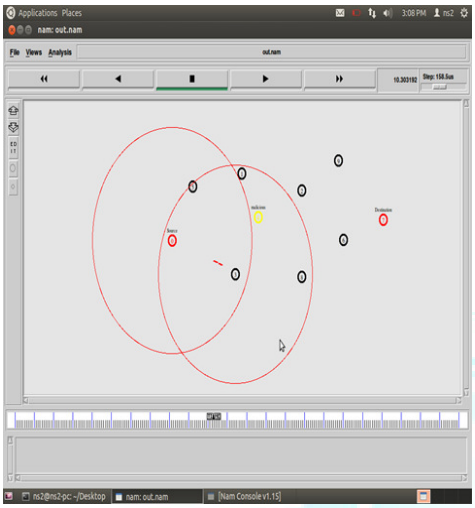
The software which going to be used in this project is Network simulator version 2.Ns-2 is a discrete event simulator targeted at networking research. Ns-2 provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks.

Outputs:

1.detection of malicious node and packet loss:



2.finding alternate route:



V. CONCLUSION

Here by we conclude that each performance will provide a detail description about the secure eaack scheme. In order to provide security digital signature is going to be included in our project as a future work. DES algorithm and RSA algorithm to be included. Thus our scheme provide a detailed comparison between various scheme and bit error are calculated in terms of packet delivery ratio.

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. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[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] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: SpringerVerlag, 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 IEEE Workshop 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 misbehaviour 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 misbehaviour 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.