# An Improvised Intrusion Detection System for MANETs – Defensive EAACK

R.Gowtham, Celeste Fatima, R.G.Gopeeka, A.Chandrasekar

***Abstract***

**MANET does not require a fixed network infrastructure. The open medium and wide distribution of nodes make MANET vulnerable to security attacks. Hence, it is crucial to develop an efficient Intrusion Detection System. In this paper, a novel system called DEAACK – Defensive Enhanced Adaptive ACKnowledgement specially designed for MANET is used. This Scheme overcomes the hurdles faced by the Watchdog scheme. Packet dropping attack has always been a major threat in security in MANET and it is overcome successfully EAACK. DEAACK proposes to use multiple key generation mechanism to eliminate forged acknowledgement packets. Using this scheme we enhance the security by dividing the keys into number of slots.**

## INTRODUCTION

MANET is a collection of mobile nodes equipped with both a wireless-transmitter and receiver that correspond with each other via bi-directional wireless links either directly or indirectly. Industrial remote access and control via wireless network becoming more and more popular these days. One of the key advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. MANET has a decentralized network 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 mission vital 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 impractical to install in scenarios like natural or human-created disasters, military differences and medical emergency. Anyway, seeing the fact that MANET is popular among mission critical applications, network security is of vital importance unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. Intrusion detection is the act of detecting surplus traffic on a network or a device. An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. Attack prevention measures, such as validation and encryption, can be used as the first line of defence for reducing the possibilities of attacks. However, these techniques have a restriction on the effects of prevention techniques in general and they are designed for a set of known attacks. They are unlikely to prevent newer attacks that are designed for circumventing the existing security measures. In this paper we are implementing the method of digital signature with multiple key generation schemes to enhance security by dividing the key into slots and sending it to the receiver. A further section in this paper is about related works, existing systems, proposed system and conclusion.

## EXISTING SYSTEM

As discussed before, due to the margins of most MANET routing protocols nodes in Mobile Ad-hoc network's finds that other nodes always cooperate with each other to relay data. This hypothesis leaves the attackers with the

opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, Intrusion Detection System (IDS) should be added to augment the security level of MANETs

## INTRUSION DETECTION SYSTEM

If MANET can detect the attackers once they get into the network, we will be able to completely eliminate the budding damages caused by compromised nodes at first time. IDSs usually act as the second layer in MANETs, and it is a great balance to existing proactive approaches. Jie et al. presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK and AACK.

## WATCHDOG

Watchdog that aims to improve throughput of net-work 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 MANETs. It is responsible for detecting malicious nodes misbehaviours in the network. Watchdog detects malicious misbehaviours by promiscuously listens to its next hop's transmission. If Watchdog node overhears that its next node fails to for-ward the packet within a certain period of time, it in-creases its failure counter. Whenever a node's failure counter exceeds a pre-defined 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 MANET IDSs are either based on or developed as an improvement to the Watchdog scheme. Watchdog scheme fails to detect malicious misbehaviours with the presence of

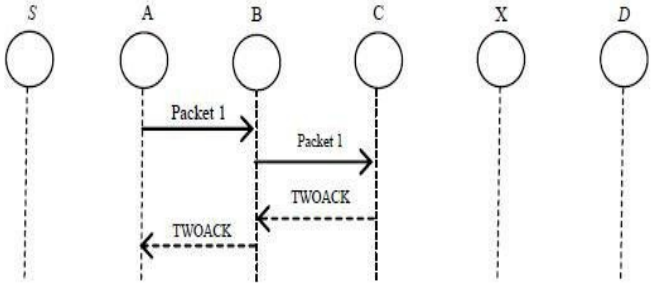
- Ambiguous Collisions
- Receiver Collisions
- Limited Transmission Power
- False Misbehaviour Report
- Collusion
- Partial Dropping

**End-to-end Acknowledgment Schemes:** Acknowledgments are sent by the end-receiver to notify the sender about the reception of data packets up to some locations of the continuous data stream. The Selective Acknowledgment (SACK) technique is used to acknowledge out-of-order data blocks. The attackers (misbehaving nodes) are assumed to be capable of performing the following tasks:

- Dropping any data packet;
- Masquerading as the node that is the receiver of its next-hop link;
- Sending out fabricated ACK packets;
- Sending out fabricated $h_n$, the key generated by the ACK packet senders;
- Claiming falsely that it's neighbour or next-hop links are misbehaving.

## TWOACK

TWOACK is neither an enhancement nor a Watch-dog based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR).



The working process of TWOACK is demonstrated in Fig. 1, 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 re-ported 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 un-wanted network overhead. Due to the limited battery power nature of MANETs, Such redundant transmission process can easily degrade the life span of the entire network.

**AACK**

It is based on TWOACK Acknowledgement (AACK) similar to TWOACK, AACK is an acknowledgement based network layer scheme which can be considered as a combination of a scheme call ACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACK. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. 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 over head, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehaviour report and forged acknowledgement packets. In fact, many of the existing IDSs in MANETs adopt acknowledgement based scheme, including TWOACK and AACK. The function of such detection schemes all largely depend on the acknowledgement packets. Hence, it is crucial to guarantee the acknowledgement packets are valid authentic .To address this concern, to adopt digital signature with multiple key generation in proposed scheme DEAACK.

**PROPOSED SYSTEM**

The Proposed approach DEAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely false misbehaviour, limited transmission power and receiver collision. In this section, we describe our proposed Defensive Enhanced Adaptive ACKnowledgement (EAACK) scheme in details. The approach described in this research paper is based on our previous work, where the backbone of EAACK was proposed and evaluated through implementation. In this work, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgement packets. DEAACK is consisted of four major parts, namely: ACKnowledge (ACK), Secure-ACKnowledge (S-ACK) Misbehaviour Report Authentication (MRA) and digital signature with multiple key generations.

**ACK**

As discussed before, 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 misbehaviour is detected. In Fig. 2, in ACK mode, node S first sends out an ACK data packet *ad*1 *P* t o the destination node D. If all the intermediate nodes along the route between node S and node D are cooperative and node successfully receives *ad*1 *P* , node D is required to send back an ACK acknowledgement packet *ak*1 *P* along the same route but in a reverse order. Within a predefined time period, if node S receives *ak*1 *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.

**S-ACK**

S-ACK scheme is an improved version of TWOACK scheme proposed by Liu *et al*. The principle is to let each three consecutive nodes

work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node. The intention of introducing SACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power As demonstrated in Fig. 8, in S-ACK mode, the three consecutive nodes (i.e. A, B and C) work in a group to detect misbehaving nodes in the network. Node A first sends out S-ACK data packet to node B. Then node B forwards this packet to node C. When node C receives, as it is the third node in this three-node group, node C is required to send back an S-ACK acknowledgement pack-et to node B. Node B forwards back to node A. If node A does not receive this acknowledgement packet within a predefined time period, both nodes B and C are reported as malicious. Moreover, a misbehaviour report will be generated by node A and sent to the source node S. 1 $P_{s\,ad\,1}$,$P_{s\,ad\,1}$, $P_{s\,ak\,1}$,$P_{s\,ak1}$ . Nevertheless, unlike TWOACK scheme, where the source node immediately trusts the misbehaviour report, DEAACK requires the source node to switch to MRA mode and confirm this misbehaviour report.

This is a vital step to detect false misbehaviour report in our proposed scheme. Detect misbehaving nodes in the network. Node A first sends out S-ACK data packet $P_{s\,ad1}$ to node B. Then node B forwards this packet to node C. When node C receives $P_{s\,ad1}$ , as it is the third node in this three-node group, node C is required to send back an S-ACK acknowledgement packet $P_{s\,ak1}$ to node B. Node B forwards $P_{s\,ak1}$ back to node A. If node A does not receive this acknowledgement packet within predefined time period, both nodes B and C are reported as malicious. Moreover, a misbehaviour report will be generated by node A and sent to the source node S. Nevertheless, unlike TWOACK scheme, 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 report in our proposed scheme.

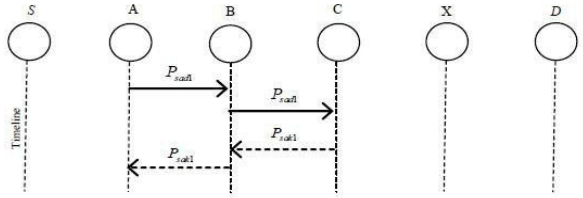



Fig.2: SACK Scheme: Node C is required to send an acknowledgement to node A

**MRA**

The Misbehaviour 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 misbehaviour 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 MANETs, it is common to find out multiple routes between two nodes. By adopting an alternative route to the destination node, we circumvent the misbehaviour 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 misbehaviour re-port and whoever generated this report is marked as malicious. Otherwise, the misbehaviour report is trusted and accepted. By the adoption of MRA scheme, DEAACK is capable of detecting malicious nodes despite the existence of false misbehaviour report.

**Digital Signature with Multiple Key Generations:**

As discussed before, DEAACK is an acknowledgement based IDS. All three parts of DEAACK, namely: ACK, SACK and MRA are acknowledgement based detection schemes. They all rely on acknowledgement packets to detect misbehaviours in the network. Thus, it is extremely important to ensure all acknowledgement packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgement packets, all of the three schemes will be vulnerable. With regarding to this urgent concern, we incorporated digital signature with multiple key generation in our proposed scheme. In order to ensure the integrity of the IDS, DEAACK requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted. Using the multiple key generation we can ensure that the key sent is not hacked by any malicious node which exist between the sender and receiver nodes. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented both DSA and RSA digital signature scheme in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

## SIMULATION RESULTS

### A. Simulation Methodologies

To better investigate the performance of EAACK under different type of attacks, we propose three scenario settings to simulate different type of misbehaviours or attacks.

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

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

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

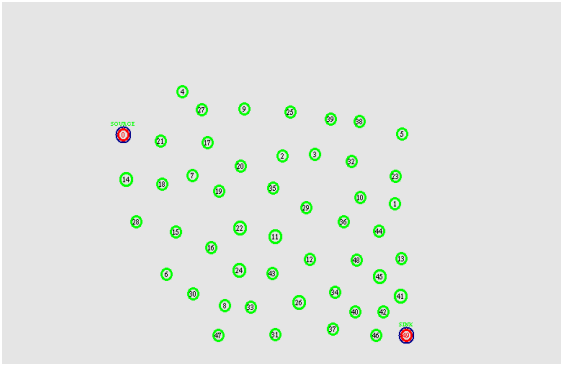


Fig.1 Declaring the source and destination nodes

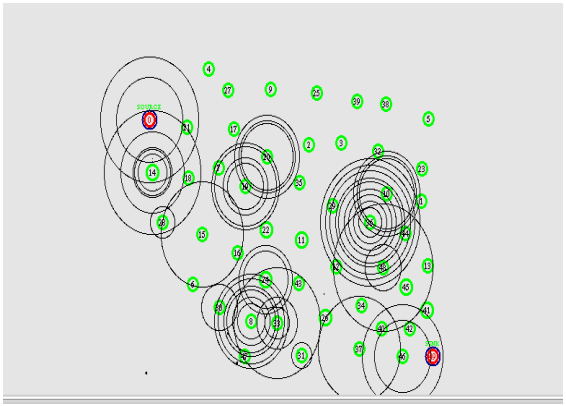


Fig.2 Broadcasting for finding the route for packet transmission.

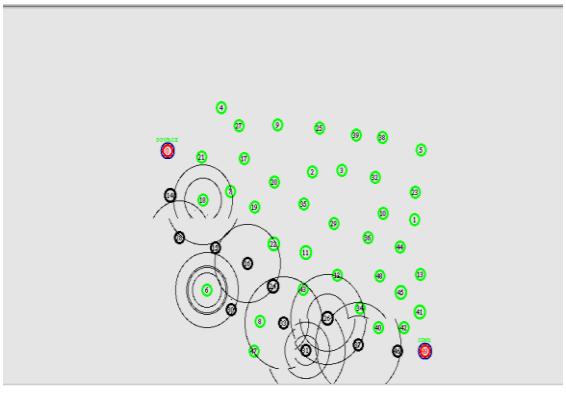


Fig.3 A path is chosen from source to destination.

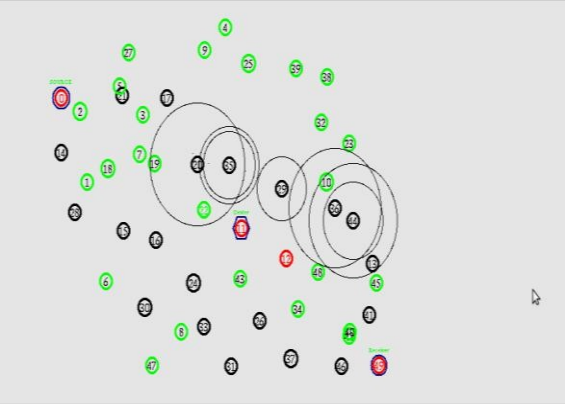


Fig.4 A centralised node is formed for monitoring the nodes and the attacker nodes are detected in the current path so searching for an alternative path without malicious nodes .

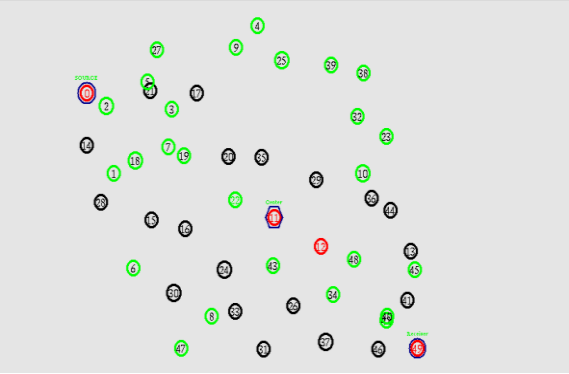


Fig.5 An alternative path is found.

**B. Simulation Configurations**

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 3GB 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 the size of 670x670m. 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 20m/s and a pause time of 1000s. UDP traffic with Constant Bit Rate (CBR) is implemented with a packet size of 512 bytes. For each schemes, we ran every network scenarios for three times and calculated the average performance. In order to measure and compare the performance of our proposed scheme, we continue to adopt the following two performance metrics:

Packet Delivery Ratio (PDR):- PDR defines the ratio of the number of packets received by the destination node and the number of packets sent by the source node.

Routing Overhead (RO):- RO defines the ratio of the amount of routing-related transmissions (RREQ, RREP, RERR, ACK, S-ACK and MRA). During the simulation, the source route broadcasts a Route REQuest (RREQ) message to all the neighbours within
its communication range. Upon receiving this RREQ message, each neighbour appends their addresses to the message and broadcast this new message to their neighbours. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocols like DSR, a Route ERR or (RERR) message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates a Route REPly (RREP) message and sends this message back to the source node by reversing the route in the RREQ message. Regarding the digital signature schemes, we adopted an open source library named Botan. This cryptography library is locally compiled with GCC 4.3. To com-pare performances between DSA and RSA scheme, we generated 1024 bit DSA key and 1024 bit RSA key for every node in the network. We assumed that both a public key and a private key are generated for each node and they were all distributed in advance. Typical size of public key and private key file is 654 bytes and 509 bytes with a 1024 bit DSA key respectfully. On the other hand, the size of public key and private key file for 1024 RSA is 272 bytes and 916 bytes respectively. The signature file size for DSA and RSA is 89 bytes versus 131 bytes respectively. In terms of computational complexity and memory consumption, we did a research on popular mobile sensors. According to our research, one of the most popular sensor nodes in the market is Tmote Sky. This type of

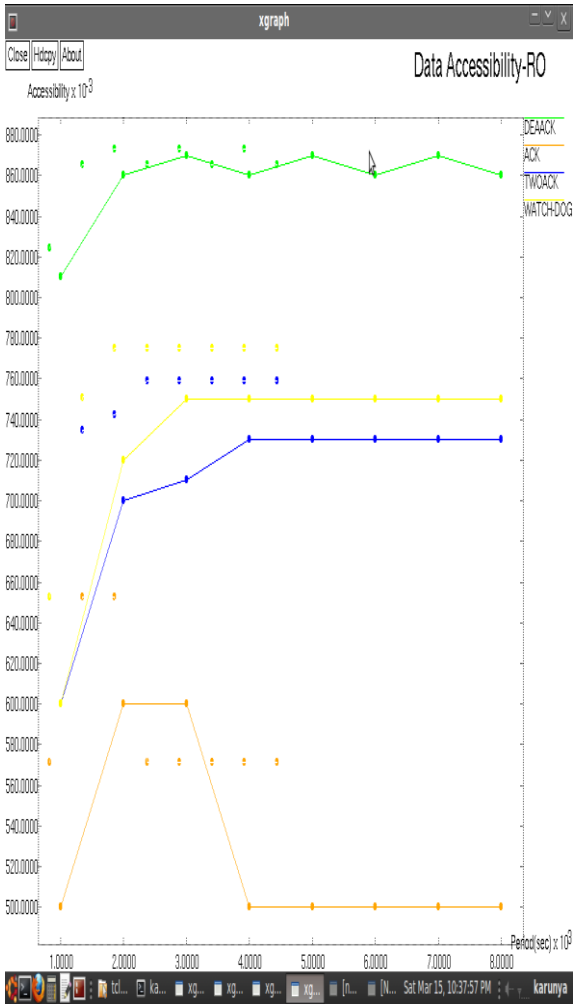



Fig.6 Simulation graph showing the data accessibility.

sensor is equipped with a TI MSP430F1611 8MHZ CPU and 1070KB of memory space. We believe this is enough for handling our simulation settings in terms of both computational power and memory space.

## CONCLUSION

Mobile Ad Hoc Network has always been prone to security attacks. Since the existing methods concentrate only on detecting the malicious nodes we are not aware of the validity of the acknowledgement packets on which we fully rely on. So to ensure to validate the acknowledgement packets we digitally sign the keys and transmit the keys. We also implement a method of generating multiple key by dividing keys into slots. This leads to maximum network security for the present scenario without the loss of network performance.

## REFERENCES

[1] R. Akbani, T. Korkmaz and G.V.S Raju. "Mobile Ad hoc Net-work Security", Lecture Notes in Electrical Engineering, vol. 127, pp. 659-666, Springer, 2012 – here1

[2]. R.H. Akbani, S. Patel, D.C. Jinwala. ―DoS Attacks in Mobile Ad Hoc Networks: A Survey‖ , the proceedings of the Second International Meeting of Advanced Computing & Communication Technologies (ACCT) , pp. 535-541, Rohtak, Haryana, India. 2012. – here1

[3]. L. Buttyan and J.P. Hubaux. Security and Cooperation in Wireless Networks. Cambridge University Press, Aug. 2007.

[4]. N. Kang, E. Shakshuki andT. Sheltami. Detecting Misbehaving Nodes in MANETs. The 12th International Conference on Information Integration and Web-based Applications & Services (iiWAS2010), ACM, pp. 216-222, November, 8-10, Paris, France, 2010.

[5]. N. Kang, E. Shakshuki andT. Sheltami. Detecting Forged Acknowledgements in MANETs. The 25th International Conference on Advanced Information Networking and Applications (AINA), IEEE Computer Society, Biopolis, Singapore, March 22-25, 2011.

[7]. V. C. Gungor, G. P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approac," IEEE Trans. on Industrial Electronics, vol. 56, no. 10, pp. 4258-4265, Oct 2009.

[8]. Adnan Nadeem, Micheal P. Howarth, ―A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks‖ , IEEE Communications Surveys & Tutorials, Vol. 5, No. 4, Fourth Quarter 2013, pgs 2027 – 2045

[9]. Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami,

Member, IEEE, ―EAACK—A Secure Intrusion-Detection system for MANETs‖ , IEEE Transactions on Industrial Electronics, Vol.60, No. 3, pg 1089-1098, March 2013

[10]. Jiwen Cai, Ping Yi, Jilan Chen, Zhiyang Wang , Ning Liu, ―An Adaptive Approach to Detecting Black Hole and Gray Hole Attacks in Ad Hoc Network‖ ,IEEE International Conference on Advanced Information Networking and Applications ,ISSN: 1550-445X,pgs 775-780,2010

[11]. Min Ji Kim, Muriel Medard, Joao Barros, ―Algebraic Watchdog: Mitigating Misbehavior in Wireless Network Coding‖ , IEEE Journal on SelectedArea in Communications,vol. 29,no.0 pg. 1916-1925,December 2011

[12]. Kashyap Balakrishnan, Jing Deng , Pramod K. Varshney, ―TWOACK : Preventing Selfishness in Mbile Ad Hoc NETworks‖ ,IEEE Wireless Communications and Networking Conference ,ISSN :1525-3511,pgs 2137-2142 Vol. 4,March 2005

[13]. Sumit More, Mary Matthews, Anupam Joshi, Tim Finin, ―A Knowledge – Based Approach To Intrusion Detection Modeling‖ , IEEE CS Security and Privacy Workshops, 2012

[14]. V. Khadilkar, J. Rachapalli, and B. Thuraisingham, ―Semantic web implementation scheme for national vulnerability database,‖ Univ. of Texas at Dallas, Tech. Rep. UTDCS-
01-10, 2010.

[15]. V. Mulwad, W. Li, A. Joshi, T. Finin, and K. Viswanathan, ―Extracting Information about Security Vulnerabilities from Web Text,‖ in Proceedings of the Web Intelligence for Information Security Workshop. IEEE Computer Society Press, August 2011.