A STUDY ON EFFECTIVE APPROACH FOR INTRUSION DETECTION IN MANETS

Ayesha Unnisa [1], G. Narayana[2], T. Shesagiri[3]

[1] *M.Tech, Department of Computer Science Engineering, J.B.R.E.C, Hyderabad (India)*

[2] *Professors, Department of Computer Science Engineering, J.B.R.E.C, Hyderabad (India)*

[3] *Associate Professor, Department of Computer Science Engineering, J.B.R.E.C, Hyderabad (India)*

ABSTRACT

Now a day's most of the people are moving form wired to wireless networks. Among the wireless networks MANETS are being mostly being used. Some of the features of MANETS are that it does not require any fixed infrastructure, self-configuring ability, dynamic topology and decentralized network. Due to its features MANETS can be used in a military and emergency recovery situations .In MANETS the nodes can work both as transmitter and receiver, can communicate with each other directly and indirectly or depend on neighboring nodes to relay their messages. One of the primary concerns related to ad hoc network is to provide a secure communication among mobile nodes in a hostile environment. The ad hoc networks can be easily reached by malicious attackers so it is vital to address its security issue. In this paper we propose a new intrusion detection mechanism EAACK specially designed for MANETS which uses ACK, S-ACK and MRA methods .The acknowledgment packets are being protected using digital signature and detects malicious nodes based on their malicious behavior.

Keyword: Mobile Ad Hoc Network (MANET), Intrusion Detection, Digital Signature, Digital Signature Algorithm, Enhanced Adaptive Acknowledgment (EAACK).

I. INTRODUCTION

Mobile Ad hoc networks or MANETs are the category of wireless networks which do not require any fixed infrastructure or base stations. They can be easily deployed in places where it is difficult to setup any wired infrastructure. There are no base stations and every node must co operate with each other in forwarding packets in the network. Thus, each node acts as a router which makes routing complex when compared to Wireless LANs, where the central access point acts as the router between the nodes.

A sensor network is a special category of ad hoc wireless networks which consists of several sensors deployed without any fixed infrastructure. The difference between sensor networks and ordinary ad hoc wireless is that the sensor nodes may not be necessarily mobile. Further, the number of nodes is much higher than in ordinary ad hoc networks. The nodes have more stringent power requirements since they operate in harsh environmental conditions.

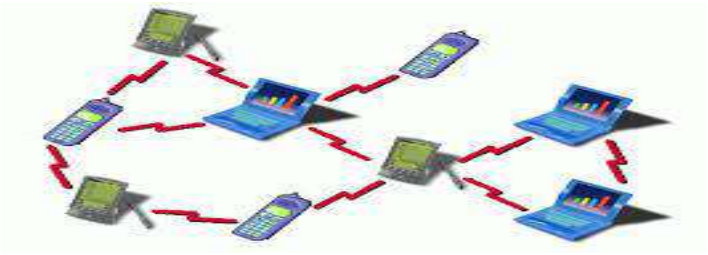

Fig-1 MANETs

1.1 Advantages Of Mobile Ad Hoc Networks

1.1.1 Low cost of deployment*:* As the name suggests, ad hoc networks can be deployed on the fly, thus requiring no expensive infrastructure such as copper wires, data cables, etc.

1.1.2 Fast deployment: When compared to WLANs, ad hoc networks are very convenient and easy to deploy requiring less manual intervention since there are no cables involved.

1.1.3 Dynamic Configuration*:* Ad hoc network configuration can change dynamically with time. For the many scenarios such as data sharing in classrooms, etc., this is a useful feature. When compared to configurability of LANs, it is very easy to change the network topology.

1.2 Intrusion Detection System

Intrusion detection can be defined as a process of monitoring activities in a system which can be a computer or a network. The mechanism that performs this task is called an Intrusion Detection System

II. PROBLEM DEFINITION

We mainly describe the existing approach, namely, the Watchdog to detect the misbehaving nodes. Watchdog aims to improve throughput of network with the presence of malicious nodes. The watchdog scheme is consisted of two parts, namely Watchdog and Path rater. Watchdog serves as an intrusion detection system for MANETs. It is responsible for detecting malicious nodes misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. The Watchdog-IDS fails to discover malicious nodes in the following situations: 1) ambiguous collisions 2) receiver collisions 3) limited transmission power 4) false behavior report 5) collusion and 6) partial dropping

2.1 Existing System

Security has become a most important service in Mobile Adhoc Network (MANETs)[5], Zhou and Haas have proposed using threshold cryptography for providing security to the network. To secure an ad hoc network, the following attributes are to be considered: availability, authentication and key management, confidentiality, integrity, non-repudiation, and scalability. In order to achieve this goal, the security solutions for each layer which are providing complete protection for MANETs are to be described.

There are five main layers on the network, as follows:

Application layer is used for detecting and preventing viruses, worms, malicious codes. Transport layer: is used for authenticating and securing end-to-end communication through data encryption, Network layer does the job of protecting the ad hoc routing and forwarding protocols. Link layer is used for protecting the wireless MAC protocol and providing link-layer security support and last the physical layer is used to prevent signal jamming,

denial-of-service attacks. Intrusion Detection System (IDS) should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at first time. IDSs usually act as the second layer in MANETs, and it is a great complement to existing proactive approaches and presented a very thorough survey on contemporary IDSs in MANETs. The existing approach, namely, the Watchdog to detect the misbehaving nodes. Watchdog aims to improve throughput of network with the presence of malicious nodes. The watchdog scheme is consisted of two parts, namely Watchdog and Pathrater. Watchdog works as an intrusion detection system for MANETs. It is responsible for detecting malicious nodes misbehaviors in the network.

2.2 Watchdog Scheme

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. 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 either based on or developed as an improvement to the Watchdog scheme.

The Watchdog-IDS fails to discover malicious nodes in the following situations: 1) ambiguous

Collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion and 6) partial dropping.

Intrusion Detection System must be added to enhance the security level of MANETS.

2.3 TWOACK

TWOACK is neither an enhancement nor a Watchdog 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).

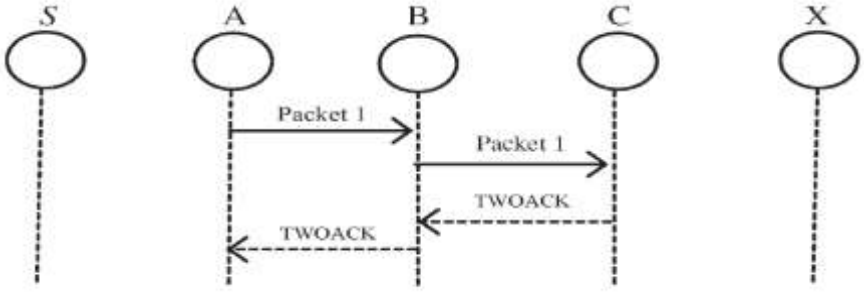

Fig-2: TWO ACK

The working of the TWO ACK scheme is as follows in Fig. 2, 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 MANETs, Such redundant transmission process can easily degrade the life span of the entire network.

2.4 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 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 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, we adopt digital signature in proposed scheme EAACK.

III. PROPOSED METHOD

Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely false misbehavior, limited transmission power and receiver collision. In this section, we discuss these three weaknesses in details. In a typical example of receiver collisions, demonstrated in Fig. 3 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.

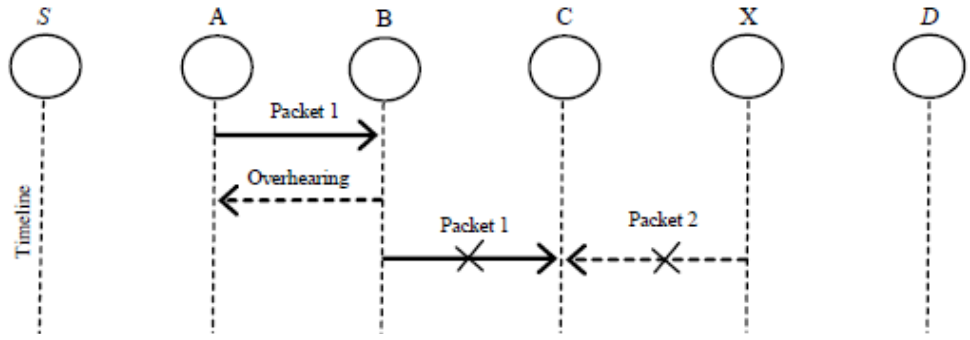

Fig-3 Receiver Collision

In 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. 4

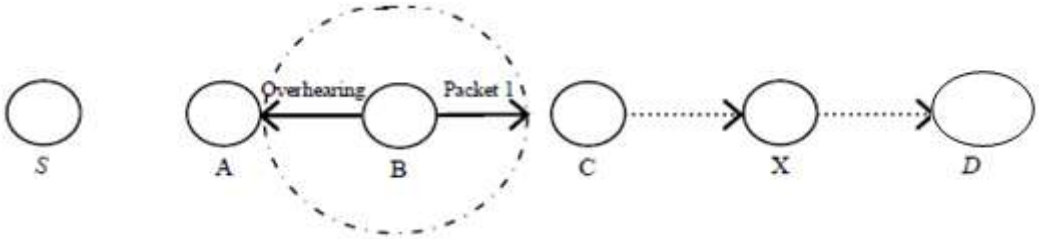

Fig-4 Limited transmission power

In the 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. 5. 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 a new intrusion detection system specially designed for MANETs, which solves receiver collision, limited transmission power, and also the false misbehavior.

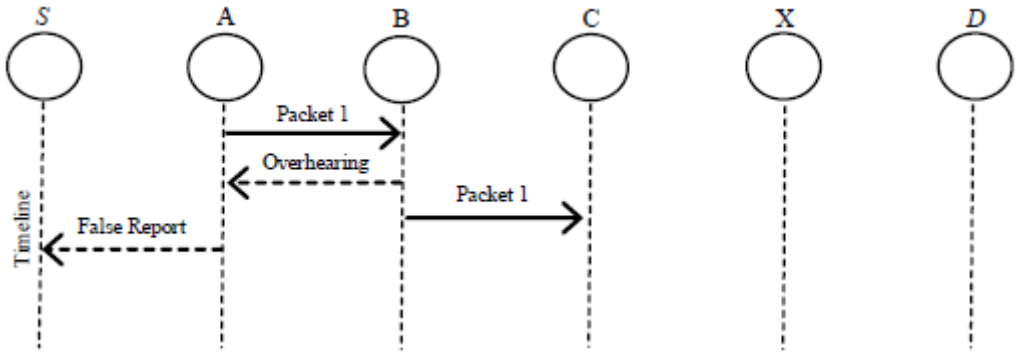

Fig-5 False Misbehavior Report: Node A Send Back Misbehavior Report Even Node B Forwarded The Packet To Node C

IV. METHODOLOGY

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). It uses the ACK and TWO ACK scheme and integrate digital signature for the acknowledgement packets. In order to distinguish different packet types in different schemes to include a 2-b packet header in EAACK. According to the Internet draft of DSR [7], there is 6 b reserved in the DSR header. In EAACK, use 2 b of the 6 b to flag different types of packets. In this secure ID, 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.

4.1 ACK

ACK is basically an end-to-end ACK IDS. It acts as a part of the hybrid IDS in EAACK, aiming to reduce network overhead when no network misbehavior 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 D are 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.

4.2 S-ACK

It is an improved extension of the TWOACK IDS [6] incorporating digital signature. 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.

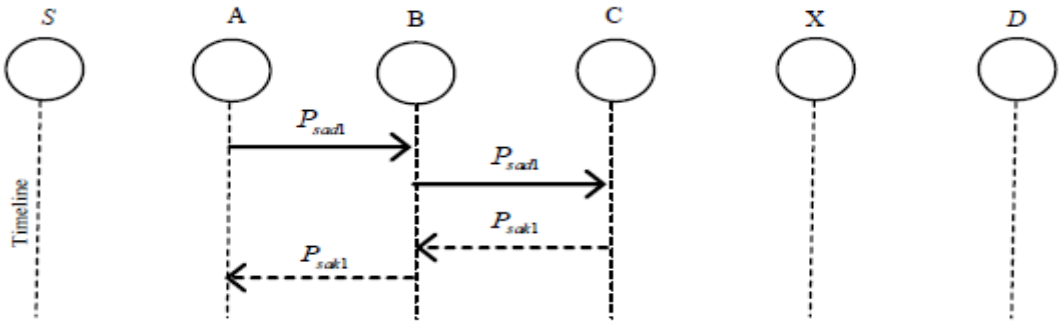

Fig-6 S-ACK scheme: Node C is required to send back an acknowledgment packet to node A.

The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

4.3 MRA

Unlike the TWOACK IDS, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior. The MRA field is designed to tackle the weakness of Watchdog when it fails to detect misbehaving nodes. The false misbehavior 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. 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 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.

4.4 Digital Signature

EAACK is an acknowledgment-based IDS. All three methods of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on ACK packets to detect misbehaviors 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 integrate digital signature in secure IDS. In order to ensure the integrity of the IDS, EAACK requires all ACK packets to be digitally signed before they are sent out and verified until they are accepted [1].

The signature size of DSA is much smaller than the signature size of RSA. So the DSA scheme always produces slightly less network overhead than RSA does. However, it is interesting to observe that the Routing Overhead differences between RSA and DSA schemes vary with different numbers of malicious nodes. The more malicious nodes there are, the more ROs the RSA scheme produces. Assume that this is due to the fact that more malicious nodes require more acknowledgment packets, thus increasing the ratio of digital signature in the whole network overhead. With respect to this result, find DSA as a more desirable digital signature scheme in MANETs [1]. The reason is that data transmission in MANETs consumes the most battery power. Although the DSA scheme requires more computational power to verify than RSA, considering the tradeoff between battery power and performance, DSA is still preferable [1].

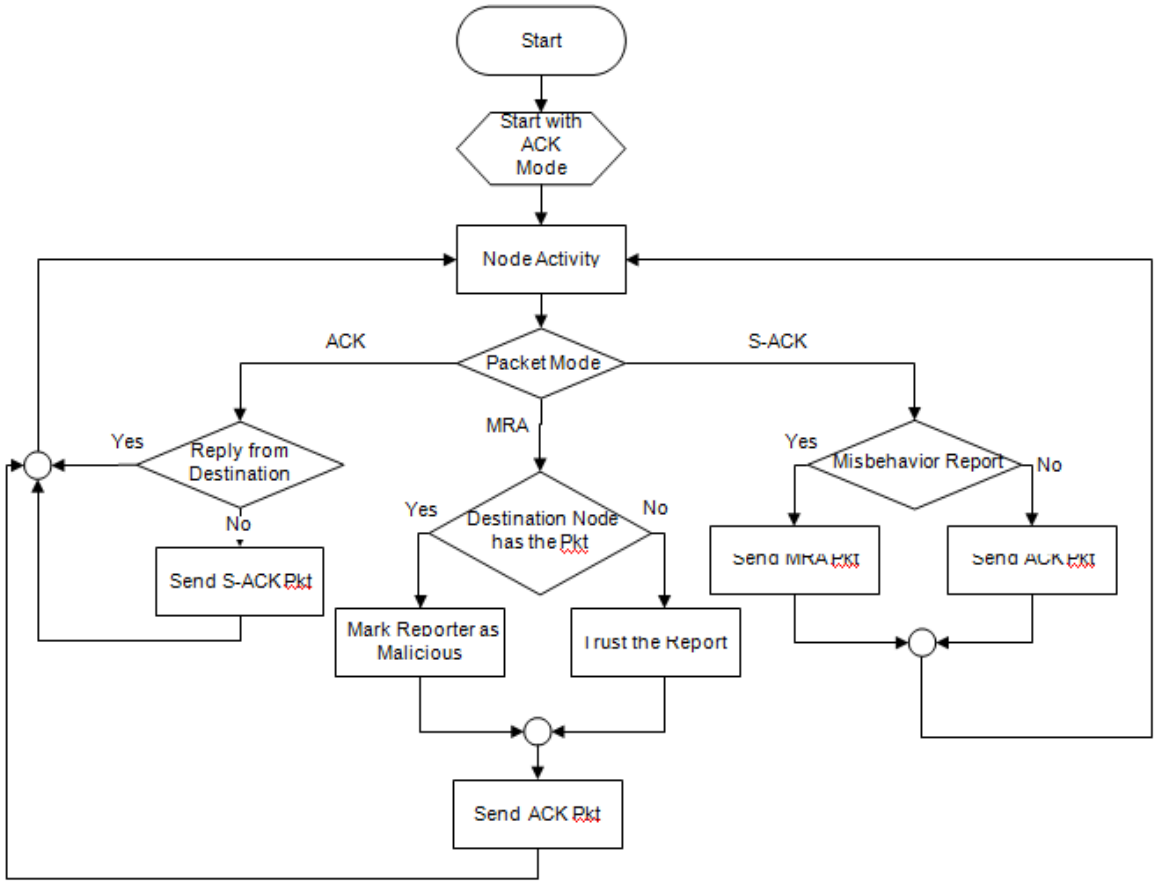

Fig-7 A. System Flow of EAACK

V. CONCLUSION

In this paper, a comparative study of Secure Intrusion- Detection Systems (SIDS) for discovering malicious nodes and attacks on MANETs is presented. Due to some of the characteristics of MANETs, prevention mechanisms alone are not adequate to manage the secure networks Therefore, security was always the major threat for MANETS so intrusion detection must be designed to address its security issues for MANET's .So in our proposed system a novel IDS (EAACK) was designed using digital signature. All three parts of EAACK, namely: ACK, SACK and MRA acknowledgement based detection schemes. They all rely on acknowledgement packets to detect misbehaving nodes in the network. Thus, it is extremely important to ensure all acknowledgement packets in EAACK are authentic and untainted .EAACK requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted. 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 was to find the most optimal solution for using digital signature in MANETs. Although the DSA scheme requires more computational power to verify than RSA, considering the tradeoff between battery power and performance, DSA is still preferable [1].

REFERENCES

[1] EAACK – A Secure Intrusion Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and TarekR.Sheltami, Member, IEEE.

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

[3] 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.

[4] T. Anantvalee and J. Wu. *A Survey on Intrusion Detection in Mobile Ad hoc Networks. In Wireless/Mobile Security*, Springer, 2008.

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

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, L. Benini, "Modeling and Optimization of a Solar Energy Harvester System for Self-Powered Wireless Sensor Networks," IEEE Trans. on Industrial Electronics, vol. 55, no. 7, pp. 2759-2766, July 2008.

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