IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 10, October 2015.
www.ijiset.com
ISSN 2348 – 7968

Secured Algorithm to Protect Sensor Nodes in Wireless Sensor Networks

Rajalakshmi Murugesan[1], Dr C.Parthasarathy[2] and Indrajith Ramasamy Venugopal[3]

[1] CSE, SCSVMV
Kancheepuram, Tamilnadu, India

[2] IT, SCSVMV
Kancheepuram, Tamilnadu, India

[3] CSE, Sri Karpaga Polytechnic College,
Kancheepuram, Tamilnadu, India

Abstract

Advance in technology introduces new security application areas for sensor node protection. We propose a security approach for node that uses secret key cryptography and key management along with encryption support. A salient feature of our approach is that a secret key is stored in the source code of every node to protect the other keys in its memory. Even the node is captured physically; the sensitive information cannot be retrieved. Our key selection protocol uses the node ID and some basic rotate and multiplication function to select the key for current data transmission. Because of this dynamic key selection, our approach identifies the replay attack, DoS attack and Sybil attack. Our simulation results shows that our security mechanism efficiently controls various attacks with lower resource requirements and the network resilience against node capture is substantially improved. WSN are becoming significantly vital to many applications, and they were initially used by the military for surveillance purposes. One of the biggest concerns of WSNs is that they are very defence less to security threats. Due to the fact that these networks are susceptible to hackers; it is possible for one to enter and render a network. The scheme is based on probability key sharing among sensor nodes of a random graph and incorporates a threshold property. Uncompromised nodes in a sensor network are secure provided that an adversary compromises less than a threshold-number of nodes. We describe the details of our algorithm and briefly compare it with other proposed schemes.

Keywords: *Cryptography, key, ,security algorithm,WSN.*

1. Introduction

WSNs are rapidly growing in popularity. Applications of SN that have emerged include habitat monitoring [1], robotic toys [2], and battlefield monitoring [3]. A wide range of applications are emerging, including location aware SN in the home and office, assistive technology for biomedical sensing, and outdoor deployments of SN to monitor storms, oceans, and weather events. For military deployments, security is essential to protect the routing infrastructure and packet data from threats such as eavesdropping, tampering, denial-of-service (DOS) attacks, and the physical compromise of sensor nodes deployed into enemy territory.

The research challenge is to secure the routing infrastructure against such threats given the severe resource constraints imposed by WSN. WSN consist of individual sensor nodes that are highly resource-constrained in terms of their limited energy lifetime, modest CPU, and scant memory [2, 8]. While it has been demonstrated that symmetric key cryptography can be implemented on today's wireless sensor platforms [5,12], initial results indicate that public key cryptography remains out of reach for today's SN due the compute-intensive nature of public key methods [12]. Prior work in securing WSN therefore focuses on exploiting symmetric key-based techniques for achieving authentication, data integrity, and confidentiality. As a result, a key focus of this paper concerns security obtained through symmetric key cryptography.

A notable feature of the architecture of a wireless sensor network is its hierarchy, rooted in a base station. As shown in Figure 1, a wireless sensor network often collects and relays data to a back-end server via a gateway or base station. The base station is typically resource-rich in terms of its computational ability, storage capacity, and energy lifetime compared to individual sensor nodes. A base station will have capabilities on the order of a laptop or laptop-equivalent and will be capable of both wired connectivity to the Internet as well as wireless connectivity

ISSN 2348 – 7968

to the sensor network. In some cases, the base station may be mobile, situated on top of a roving van or command vehicle, or may have limited mobility enough to be guided to an opportune location in the sensor network topology. A fundamental assumption of this paper is that the sensor network architecture conforms to the base station-rooted hierarchy shown in Figure 1. Prior work in securing SN given a base station-rooted topology includes the SPINS suite of security building blocks [5], fault tolerant routing [9], securing of TinyOS routing as well as directed diffusion [10], and the INSENS secure routing system [12]. Prior work in securing ad hoc networks given peer-to-peer routing includes SEAD [6] and Ariadne [7], which both utilize symmetric key schemes, as well as a number of public key techniques that are too costly for today's SN [15, 16, 17, 18].

Given a base station architecture and symmetric key cryptography, this paper considers strategies for securing the sensor network against a variety of threats that can lead to the failure of the base station, which represents a central point of failure. Prior work that has focused on securing the routing between sensor nodes has assumed that the base station is sufficiently powerful to defend itself against security threats. In contrast, this paper considers that the base station itself may be vulnerable. As a result strategies must be implemented throughout the sensor network to withstand attacks that can lead directly or indirectly to the failure of the base station. As shown in Figure 1, we consider three strategies for securing the sensor network against base station failure. First, as shown in Figure 1a), multipath routing to *multiple* destination base stations is analyzed as a strategy to provide tolerance against individual base station attacks. This strategy is considered both for the route discovery phase as well as the data routing phase. We also analyze the extent to which the number of base stations enhances the resilience of the network. Second, Figure 1b) illustrates confusion of address and identification fields in packet headers via hashing functions. This approach is designed to disguise the location of the base station and thereby counter threats from a passive observer who would eavesdrop on packet headers, especially the source, destination and type fields, in order to infer and trace back the location of the base station. Third, Figure 1c) depicts the relocation of the base station in the network topology. We analyze the extent to which base station mobility and placement can affect the resiliency of the network and mitigate the scope of the damage inflicted by a malicious sensor node. The strategies studied in this paper are limited to the particular kinds of threat models outlined above. Our objective is not to claim that these strategies withstand all manner of attacks, e.g. wormhole [23] attacks, or apply to all SN, e.g. mobile SN in which all sensor nodes move, not just the base station.

In Sections 2 and 3, the strategy of multipath routing to *multiple* destination base stations has been considered. Section 2 describes a route discovery protocol in a wireless sensor network in the presence of multiple base stations. Route discovery protocol ascertains the topology of a wireless sensor network after the sensor nodes are deployed. This section describes the design of this protocol, analyzes its resilience against different type of security attacks, and presents performance measurements from a simulated prototype to illustrate the power of multiple base stations during route discovery. Section 3 describes a secure and intrusion-tolerant data routing protocol that exploits multiple redundant routes to different base stations. This section illustrates the resilience of a wireless sensor network comprising of multiple base stations against sensor node compromises and base station failures via performance measurements from a simulated prototype. Protocols described in these two sections are based on INSENS secure routing mechanism [12].

In Section 4, the strategy of confusion of address and identification fields in packet headers via hashing functions has been considered. This section details how the location of the base station is disguised via confusion of identification fields as well as relocation of the base station. In Section 5, the strategy of relocating base stations has been considered. Different base station placement strategies, so as to improve the resilience of the sensor network against attacks on base stations and sensor nodes. Section 6 discusses the related work, Section 7 provides a discussion and future research directions, and finally, Section 8 concludes the paper.

To test the performance of the three strategies, we have simulated WSN in ns2[19] simulator. We use the following parameters in most of the experiments described in this paper. For a random network topology, we generate 200 nodes, and put them in a 2500 X 2500 m^2 square area. For grid network topology, we generate 14 X 14 nodes, and put them in a 2860 X 2860 m^2 square area. For each experiment, we randomly generate 30 to 50 network topologies. The results shown in various graphs in the paper are average values of each test.

2. MULTIPLE BASE STATIONS: ROUTE DISCOVERY

A route discovery protocol ascertains the topology of the sensor network. Our route discovery protocol is based on INSENS route discovery protocol [12]. INSENS provides support for intrusion-tolerant routing in wireless sensor network. It builds multiple redundant paths between sensor nodes and a base station to bypass intermediate compromised nodes. In addition, INSENS limits DOS-style flooding attacks, prevents false advertisement of

ISSN 2348 – 7968

routing and other control information, and is designed for *resource-constrained* wireless sensor network. In particular, INSENS ensures that a single compromised node can only disrupt a localized portion in the network, and cannot bring down the entire sensor network. While INSENS has several important useful features, it suffers for a serious drawback. It assumes that the base station cannot fail or be isolated from the network by malicious compromised nodes. This assumption may not hold under several scenarios. For example, if an adversary discovers the location of a base station, it can isolate it from the rest of the network by simply jamming the communication medium in its neighborhood. In this paper, we overcome this drawback by accommodating multiple base stations that cooperate with one another to build a robust wireless sensor network. In particular, we consider a redundant base stations model of wireless sensor network, and design protocols to build redundant routing mechanisms in such a network. These protocols preserve all the good features of INSENS, and in addition provide support for tolerating failure of one or more base stations.

In particular, our route discovery protocol adheres to the following design principles. First, to prevent DOS-style flooding attacks, individual nodes are not allowed to broadcast to the entire network. Only the base stations are allowed to broadcast. Base stations act as gateways to the wired world, e.g. a satellite uplink connecting to terrestrial networks. Authentication of the base stations is achieved via one-way hashes, so that individual nodes cannot spoof the base station and thereby flood the network. Unicast packets must first traverse through a base station, thereby preventing DOS/DDOS broadcast attacks.

Second, to prevent advertisement of false routing data, control routing information must be authenticated. A key consequence of this approach is that the base stations always receive knowledge of the topology that is correct, though it may only represent a partial picture due to malicious packet dropping. Third, to address resource constraints, 1) symmetric key cryptography is chosen for confidentiality and authentication between the base stations and each resource-constrained sensor nodes, since it is considerably less compute-intensive than public key cryptography, and 2) the resource-rich base station is chosen as the central point for computation and dissemination of the routing tables. Fourth, to address the notion of compromised nodes, redundant multipath routing is built to achieve secure routing. The goal is to have disjoint paths, preferably to different base stations so that even if an intruder takes down a single node or path, secondary paths will exist to forward the packet to the correct destination. Route discovery is subdivided into two rounds. In the first round, the base stations flood (limited flooding)

a *request message* to all the reachable sensor nodes in the network. In the second round, each sensor node sends its neighborhood topology information back to two different base stations using a *feedback message*.

2.1 Route Discovery: Route Request

Whenever there is a need to construct the forwarding tables of all sensor nodes, a central node directs all base stations to initiate the first round of the route discovery protocol. Each base station initiates a *request message* by broadcasting it to all its neighbors. When a sensor node receives a request message initiated by base station *b* for the first time, it forwards (broadcasts) this request message. This request message includes a path from the base station *b* to *x*. As this request message is forwarded downstream in the network, each node appends its identity in the path. On receiving a request message, a node *x* also records the identity of the sender of this message in its neighbor set. A node may receive a request message initiated by base station *b* many times. However, it forwards this request message at most once. When a node receives another request message initiated by *b*, the identity of the sender is added to its neighbor set, but the request is not rebroadcast. This implies that if there are *n* base stations, a node may forward up to *n* request messages, each initiated by a different base station. To further limit the scope of flooding of request messages, we include a protocol parameter (an integer) that dictates the maximum number of request messages a node may forward. For example, Figure 2(a) shows the forwarding of request messages when the value of this parameter is 3.

A malicious node in the network can attempt to launch several attacks in this round. First, it can attempt to spoof the base station by sending a spurious request message. Second, it can include a fake path in the request message it forwards. Third, it may not forward a request message, or launch a DOS attack by repeatedly sending several request messages. We adopt the security mechanisms of INSENS to counter these attacks. They require sensor nodes to be pre-configured with appropriate values. First, each base station *b* generates a sequence of numbers K_{b0}, K_{b1}, …, K_{bn} such that K), where F is a one-way function, $0 < j < n$, and K is chosen randomly. All nodes are pre-configured with function F, and final sequence values $K_{an}, K_{bn}, \ldots, K_{b0}$ of each base station, *a*, *b*, …, *m* respectively. A base station *b* transmits $K_{bn-1\ mn}$ in the first request message it initiates. Each sensor node can authenticate that this message originated from base station *b* by verifying $K_{bn-1} = F(K_{bn\ bj+1})$. In general, a base station *b* uses K route discovery phase. As shown in [12], this mechanism allows a sensor node to authenticate that a request message it received indeed originated from a legitimate base station. This mechanism ensures that a

ISSN 2348 – 7968

malicious node cannot spoof a base station, and cannot launch DOS attacks by replaying earlier (legitimate) request messages. However, it remains possible that a malicious node could flood a modified request message using the *current* sequence number from a valid request message just sent out by the base station. In such an attack, called a rushing attack [14], an attacker tries to propagate a spurious message before the base station can propagate its own valid message. This attack is confined to the local subtree of nodes below the malicious node. Damages inflicted due to this attack are further reduced by deploying multiple base stations. A node that receives a spurious request message first is still likely to get a valid request message initiated by some other base station. As we will see later, this will enable this node to eventually communicate with at least one base station.

The second mechanism that we use to defend against intrusions is a keyed MAC algorithm. Each sensor node is configured with a separate secret key that is shared only with the base station. This keyed MAC is used to preserve the integrity of control information included in a request message. The overall effect of these security mechanisms is that a malicious node can attack in the first round only by localized flooding, by not forwarding a request message, and by sending fake path in the request which is later on detected in the second round. The latter two attacks will result in some of the nodes downstream from the malicious node not getting a request message or not being able to forward their feedback message to the base station in the second round. Again, a malicious node may be able to compromise a small number of nodes in its vicinity by employing these types of attacks, but cannot jeopardize the security of the complete network.

2.2 Route Discovery: Route Feedback

In the second round, each sensor node sends its local connectivity information (a set of identities of its neighbor nodes as well as the path to itself from a base station *b*) back to the base station *b* using a *feedback* message. A separate feedback message is sent to every base station whose request message was forwarded in the first round. The mechanism used to send feedback messages to different base stations is same. So, for simplicity, we will concentrate on sending a feedback message to just one base station in the following discussion. After a node has forwarded its request message in round one, it waits a certain timeout interval before generating a feedback message. This interval allows a node to listen to the local broadcasts of its neighbors, who will also be forwarding the same request message. A node will hear the request messages from its upstream, peer and downstream neighbors. A feedback message containing neighbor list and path to b is propagated to b using the reverse path taken by the request message initiated by b. The integrity of the topology data returned to a base station by each node in its feedback message is protected by a keyed MAC applied over neighbor list, path, and some other control information. This MAC ensures that a base station will construct a correct topology, though it may be incomplete due to malicious nodes that may drop or tamper with feedback messages. The messages that reach the base station are guaranteed after verification to be correct and secure from tampering.

A malicious intruder could still launch several attacks. First, an intruder could launch a DOS-style attack and send multiple feedback messages to each of its upstream neighbors. Second, an intruder could eavesdrop and learn topology information. To address the first DOS-style attack, we employ two defense mechanisms: (1) To prevent repetitive transmissions of a feedback packet from the same originating node, all nodes follow the policy of not forwarding duplicate feedback messages; and (2) use rate control to prevent transmissions of feedback packets from many thousands of phantom originating nodes. To provide confidentiality against eavesdropping by a malicious node, the path and neighbor information is encrypted using the originating node *x*'s secret key, with the caveat that the identity field of the originating node in the path is left unencrypted.

The overall effect of these security mechanisms is that a malicious node is limited in the damage it can inflict, whether attacking by DOS attack, by not forwarding a feedback message or by modifying the neighborhood information of nodes, which can be detected at the base station. The rate-controlled DOS attack will affect upstream nodes, but only in a limited way. The latter two attacks will result in some of the nodes downstream from the malicious node not being able to provide their correct connectivity information to the base station. Though a malicious node could launch a battery-drain attack by persistently sending spurious feedback messages at the rate-controlled limit, such an attack would still affect a limited number of upstream nodes. In summary, a malicious node may be able compromise only a small number of nodes in its vicinity using these attacks.

2.3 Performance Evaluation of Route Discovery

As mentioned earlier, a malicious node may be able to compromise a small set of nodes in its vicinity during route discovery. We have performed a set of experiments to measure the extent of damage a malicious node can cause during route discovery. We have simulated two types of attacks a malicious node may launch. In the *passive attack*, a malicious node either drops feedback

ISSN 2348 – 7968

messages or modifies the neighbor information in the feedback message before forwarding (recall that this tampering is later on detected by a base station). The effect of passive attack is that some of the nodes may not be able to convey their connectivity information to the base station and hence will not be included in the network topology constructed by the base station.

In the active attack, a malicious node launches a DOS attack during the second round of route discovery protocol. Figure 3 shows the result of launching active and passive attacks. The x-axis in this graph records the maximum number of nodes that may be compromised by a single malicious node, and the y-axis records the number of such (malicious) nodes. For example, about 34% of the sensor nodes can disable only 5% of the nodes in the network by launching a DOS attack when three base stations are deployed. The numbers reported in this figure are averaged over 100 different randomly generated topologies of 100 nodes distributed over a 2000 X 2000 m_2 space. In case of active attack, we have calculated this damage by counting all the nodes downstream from the malicious node, its neighbors, and the neighbors' downstream nodes that do cannot reach any base station. In case of passive attack, we have calculated this damage by counting all the nodes downstream from the malicious node that cannot reach any base station.

We make three observations from this figure. First, as expected, an active attack compromises more nodes than the passive attack. Second, multiple base stations improve resiliency of the protocol from both passive and active attacks during route discovery. The main reason for this is that a single malicious node can successfully block a set of nodes from a base station if there is only one base station. However, if there are multiple base stations, it becomes extremely difficult for this malicious node to block nodes from all base stations. Finally, there is a catastrophic scenario when there is a single base station. There exists a set of nodes that can bring down the entire network. The reason for this is that the nodes in the vicinity of the lone base station can isolate it from the network by simply launching a DOS attack. Presence of multiple base stations eliminates this catastrophic scenario.

3. Related Work

3.1 Key Management

The essential requirement for secure data communication is a pair of secret keys. After the initial deployment of a sensor node, the secret key is required to communicate with the neighboring nodes. This phase where the secret key is established for a newly deployed sensor node is known as "Key pre-distribution". But the sensor resource constraints like limited power, limited computation ability or low memory make this process very difficult.

There are several key establishment schemes proposed by several researchers. The pre-distribution scheme can be deterministic or probabilistic. Apart from that there are In-situ key establishment schemes also. In the key pre-distribution schemes, before the deployment, each sensor node contains the keys or keying information. As the network topology is very much unpredictable to any sensor node before deployment, the extra information regarding key is required here. This uncertainty may hamper the performance of the key predistribution schemes [6]. Eschenauer and Gligor [2] proposed that every sensor node will have random pre-distribute keys loaded in it before the deployment. These keys will be selected from a large pool of symmetric keys. At the time of communication, the two sensor nodes search that whether they have any common key or not and if found, they share the key. If common key is not found, then they establish a path key. But in this scheme, the attackers may gather the idea and prepare the total key pool after considering several sensor nodes. Chan et al [7] proposed a scheme where two nodes require $q > 1$ number of common keys for establishing a shared key. The problem in this scheme is that as more than one pair of nodes may know the keys, so the key may be revealed by capturing a node. Besides these, two random key space schemes have been proposed by Du et al [8] and Liu and Ning [9]. First one uses symmetric matrices to define the key space and second one uses symmetric polynomials. The sensors, which want to communicate, compute the shared key if they have keying information from the same key space. But, modular multiplications make the schemes expensive in terms of computation, which is a constraint in sensor node. Another random key scheme is proposed by Chan and Perrig whose name is PIKE [10]. Here two sensor nodes communicate with each other with unique pair of keys and if no shared key is present then a trusted intermediary establishes the key.

Another type of key management scheme is in-situ key establishment scheme. In this scheme, sensors compute shared keys with their neighbors after deployment [6]. But like the random key schemes of [8] and [9], in this scheme also, the shared key computation process is complex. Another scheme proposed by Perrig et al is SPINS [3], which uses a trusted base station to establish keys among the sensor nodes. Teymorian et al. [6] proposed a cellular automaton based key management scheme, CAB, which supports rekeying activities. In CAB, each sensor contains a small number of CAs before deployment. Using CAs, highly random pair-wise keys can be generated using simple bitwise OR and XOR operation. In addition to that, the keys can be computed on demand by sensors that have a common CA.

3.2 Secured Data Communication

ISSN 2348 – 7968

The method of secure data transmission in WSN is more difficult than other conventional wireless networks because of its constraints mentioned above. There is no adequate memory space where the variables of the asymmetric cryptosystem will be stored. As far as different type of attacks in WSN are concerned, the expected attacks in conventional wireless network like the Denial of service (DoS) attacks, time synchronization attacks, physical layer attacks, routing threats, malicious traffic injection etc. can be possible in WSN also [4].
Roy Chowdhury et al [4] proposed a cellular automaton based lightweight data authentication protocol (CADA) which not only ensures secure data transmission but also tracks malicious motes. In their protocol, the maximum workload is given to the sink keeping in the mind the limited computational capabilities of the motes.

3.3 CAKD - KEY PRE-DISTRIBUTION ALGORITHM
While developing the algorithms, we have kept in our mind the constraints of the sensor nodes that is
a) Nodes have computational constraints i.e. complex computation should be avoided
b) Nodes have small amount of memory, so huge data can not be stored in the nodes
c) Nodes get their energy/ power from battery, so extra computation will decrease the battery power as well as node power also.
Keeping these constraints in mind we have tried to develop the algorithms, which have less complex calculation, take little time also.

In a WSN, there may be several clusters of nodes. Each cluster contains a cluster head or base station which acts as server and all the motes in that cluster act as clients of that base station. If one mote wants to communicate with another

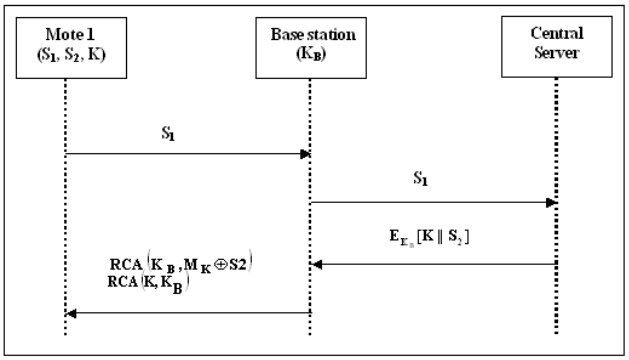

Fig. 1. Distribution of operating key of a sensor node by the base station

mote within the same cluster, then the communication is done through the base station. If one mote wants to communicate with a mote of a different cluster, then the communication is done through the base stations of the two clusters. The entire key pre-distribution operation is depicted in figure 1.
a) At the time of deployment, a new mote will contain an encrypted key (K) of 4 bytes and two unique serial numbers S1 and S2 of 3 bytes each. Every mote will have these preloaded information which will be kept by a central server. After the deployment, a new mote M1 sends the serial number S1 to its base station.
b) The base station sends the serial number S1 to the central server for the authentication. If any rouge mote sends a fake serial number, the central server can identify this.

4. Conclusions

The main purpose of this research is to propose a secure sensor node authentication protocol for WSN. The architecture of the proposed protocol consist a network administrator, a base station, large number of sensor nodes and many users. Administrator preloads the identity of the nodes or users and informs the BS. BS registers the nodes and users; and also generates the private key of all nodes or users in the network. After registration of a node by the BS, the node will now capable to send authentication request to the network and the node surrounding of requesting node will perform the authentication. Only the registered node will get The assessment through the analysis, it ensures that the protocol node authentication protocol is more secure and
energy efficient. One more important characteristics of this protocol is the reusability of IBS. If a new better version of IBS algorithm available then the protocol can easily substitute the old IBS with the new one. The new IBS may provide better performance and make more secure the protocol. The sensor network is resource constraint network having limited power. The main source of the power is the battery (AA type). More security requires more energy. As the security is main attention in this proposed protocol, so it is very important to do the proper balancing of the security and power so that the network will run for longer time without any interruption of power.
The protocol is proposed and analyzed through the theoretical analysis. It is also important to assure whether the protocol is good for the practical environment. So our works in future will be finding out more concrete solution for the node capture attack and implementing the overall protocol to monitor the actual effect in the real environment in terms of different parameters like security, energy consumption, efficiency, durability etc

References

[[1] R. Anderson and M. Kuhn, “Low cost attacks on tamper resistant devices”, In *Proceedings of the International Workshop on Security Protocols (IWSP), Lecture Notes in Computer Science(LNCS),* 1997.

ISSN 2348 – 7968

[2] D. Braginsky and D. Estrin, "Rumor routing algorithm for sensor networks", In *Proceedings of the 1 ACM International Workshop on WSN and Applications",* pp. 22-31, New York, NY, USA, 2002, ACM Press.
[3] T. Aura, P. Nikander, and J. Leiwo, "DOS-resistant authentication with client puzzles", In Revised papers from the *8 th International Workshop on Security Protocols*, pp. 170-177, Springer-Verlag, 2001.
[4] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M.B. Srivastava, "On communication security in wireless ad-hoc sensor networks", In *Proceedings of 11 th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02),* 2002, pp. 139-144.
[5] P. Albers and O. Camp, "Security in ad hoc networks: A general intrusion detection architecture enhancing trust-based approaches", In *Proceedings of the 1 st International Workshop on Wireless Information Systems, 4 th International Conference on Enterprise Information Systems*, 2002.
[6] H. Chan and A. Perrig, "Security and privacy in sensor networks", *IEEE Computer Magazine*, pp. 103-105, 2003.
[7] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J. Tang, "Framework for security and privacy in automotive telematics", In *Proceedings of the 2 nd ACM International Workshop on Mobile Commerce*, 2000.
[8] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks", In *Proceedings of the 2 ACM Workshop on Security on Ad Hoc and Sensor Networks*, Washington DC, USA, 2004. *st nd* [4] A. A. Name, "Conference Paper Title", in Conference Name, Year, Vol. x, pp. xxx-xxx.