ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

An Efficient Distributed Detection in Sensor Networks with Mobile Access under Byzantine Attacks

M.Chakka Raja[1], W.Stalin Jacob[2]
[1] P.G. Scholar, M.E Communication System, Francis Xavier Engineering College, Tirunelveli.
[2]Assistant Professor, Department of ECE, Francis Xavier Engineering College, Tirunelveli.

Abstract: Wireless Sensor Networks (WSNs) have played a vital role, and that is considered to be one of the immense and emerging technologies as there are various innovative applications both for public sector and military organizations. A serious threat is the Byzantine attack in the wireless sensor networks where the adversary has full control over some of the authenticated nodes and it can perform arbitrary behavior to disrupt the system. The byzantine attacks detection is very important to avoid the system degradation. SENMA has two types of nodes sensors and mobile access points (APs).To detect both static and dynamic Byzantine attacks in reliable data fusion in wireless sensor networks with mobile access points (SENMA) the paper uses linear q-out-of-m-rule. This rule can achieve satisfying accuracy with low false alarm rate. It can also perform malicious node detection using adaptive data fusion under time-varying attacks.
Keywords: Security in wireless sensor networks, Byzantine attacks, distributed detection

I. INTRODUCTION

A network is a group of two or more computer systems linked together. There are many types of computer networks.A wireless Access Point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself. Prior to wireless networks, setting up a computer network in a business, home or school often required running many cables through walls and ceilings in order to deliver network access to all of the network-enabled devices in the building. Sensor networks with mobile access point (SENMA) architecture for low-power and large scale sensor networks is as shown in SENMA has two types of nodes sensors and mobile access points (APs). Sensors, often deployed randomly in large quantity, are low-cost nodes with limited processing and communication capability.Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur.

1.1 Byzantine Attack

Byzantine fault tolerance is a sub-field of fault tolerance research inspired by the Byzantine Generals' Problem, which is a generalized version of the Two Generals' Problem. The objective of Byzantine fault tolerance is to be able to defend against Byzantine failures, in which components of a system fail in arbitrary ways. Correctly functioning components of a Byzantine fault tolerant system will be able to correctly provide the system's service assuming there are not too many Byzantine faulty components. A Byzantine fault is an arbitrary fault that occurs during the execution of an algorithm by a distributed system. It encompasses both omission failures (e.g., crash failures, failing to receive a request, or failing to send a response) and commission failures (e.g., processing a request incorrectly, corrupting local state, and/or sending an incorrect or inconsistent response to a request).

In a Byzantine fault tolerant (BFT) algorithm, steps are taken by processes,A faulty process is one that at some point exhibits any of the above failures. A process that is not faulty is correct. The Byzantine failure assumption models real-world environments in which computers and networks may behave in unexpected ways due to hardware failures, network congestion and disconnection, as well as malicious attacks.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

II. PROBLEM DESCRIPTION

2.1 THE Q-OUT-OF-M SCHEME

The MA would use the q-out-of-m fusion method, where it polls m out of n sensors and relies on the q-out-of-m rule for final decision making. In the q-out-of-m fusion scheme, the MA decides that an object is present if q out of them polled sensors report '1'. The main objective is to minimize the overall false alarm rate (QF) while keeping the overall miss detection (Qm) below certain predefined value β. Hence, it is desired to get the optimum parameters m and q that can achieve the objectives. It is used exhaustive search to obtain the optimal parameters at relatively small network sizes using β=0.01, and two main observations were made Observation 1: The optimal mis almost independent of the percentage of malicious nodes, and has a linear relationship with n. One possible interpretation for this is that since the polling is random, it is better to know the decision of all the nodes. This is not the case when a malicious node detection scheme is employed, as in this case the reports of malicious sensors would be discarded. Observation 2: q also follows an approximate linear function of n with different slopes depending on the percentage of malicious nodes. These observations are used to obtain sub optimal m and q for large network sizes without the need to perform exhaustive search that would be impractical as n increases.

2.2 MALICIOUS NODE ATTACK STRATEGIES

The optimal and the suboptimal scheme parameters for q-out-of-m approach consider the worst case scenario where malicious nodes always send false sensing information. These parameters (m,q) are also used for more general attacking approaches.

- Strategy 1: In this strategy, it considers that malicious nodes always report false sensing information.
- Strategy 2: The malicious nodes send false data with an arbitrary probability. This means that malicious nodes are not always reporting the false information. Hence, malicious nodes will be more difficult to be detected compared to the first strategy.
- Strategy 3: In this scheme, the malicious nodes follow a dynamic strategy to attack. It is assumed that all malicious nodes have the same probability of attack in different sensing periods.

2.3 MALICIOUS NODE DETECTIONAPPROACH

In this case benign nodes could be regarded as malicious or vice versa. To avoid this case, it assumes a maximum percentage for malicious nodes to be 30%. If the ratio of the discarded nodes exceeds this percentage, the scheme keeps updating the counters for each node without discarding any sensing report. Simulations will show that this simple malicious detection approach improves the performance significantly.

Second, in an effort to search for an easier and more flexible distributed data fusion solution that can easily adapt to unpredictable environmental changes and cognitive behavior of malicious nodes, it derives a closed-form solution for the q-out-of-m fusion scheme based on the central limit theorem. It is observed that the closed-form solution is a function of the network size, the percentage of malicious users, the malicious nodes' behavior, and the detection accuracy of the sensor nodes. It shows that under a fixed percentage of malicious nodes, the false alarm rate for both approaches diminishes exponentially as the network size increases. Finally, it proposes a simple and effective malicious node detection approach, where the malicious sensors are identified by comparing the decisions of the individual sensors with that of the fusion center. It is observed that dynamic attacks generally take longer time and more complex procedures to be detected as compared to static attacks.

III.PROPOSED MODEL

3.1 SIMPLIFIED DATA FUSION SCHEME—THE LINEAR APPROACH

3.1.1 Linear approach

This section presents a simplified q-out-of-m scheme by exploiting the linear relationship between the scheme parameters and the network size. The main idea is that this method can get the optimal scheme parameters at relatively small network sizes, and use them as reference points. These optimal (m, q) pairs for the different network sizes, Pa values, and a ratios, can be obtained and stored in a look-up table, then used to get the suboptimal scheme parameters for large network sizes. This method proposes to set m = n and use the following linear function of n to obtain q:

$$\hat{q}_{n,\alpha} = \left[q_{n_o,\alpha} + S_o(\alpha)(n - n_o) \right] \qquad (1)$$

where $S_o(\alpha)$ is the slope of the optimal q_o versus n curve at a particular attack probability given that the percentage of the malicious nodes is α, $\hat{q}_{n,\alpha}$ is the suboptimal q value at a network size n, and $q_{n,\alpha}$ is the optimal q value at a relatively

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

small network size n_0 and it serves as a reference point. Both $\hat{q}_{n,\alpha}$ and $q_{n,\alpha}$ are at α percent of malicious sensors. $\lceil x \rceil$ is the smallest integer larger than or equal to x.While the linear approach can deliver very good performance, there are chances of violating the problem constraint. Therefore, this method proposes an enhanced linear approach to guarantee that the choice of q satisfies the miss detection probability constraint.

The absence of a well-defined closed-form solution makes it difficult to adapt q based on the environmental conditions and the malicious behavior. To find q for different network settings, the slopes and the reference points should always be updated using exhaustive search. This could be tedious when the environment is fast-varying. To solve this problem, in the following section, it first derives a closed-form expression for q.

3.1.2 A Closed-Form Solution

This section derives a closed-form solution of q for the q-out-of-m fusion rule under both static and dynamic attacks. It exploits the observations of the optimal exhaustive search by setting m = n, as illustrated in the previous section. Recall that the malicious sensors have miss detection and false alarm attack probabilities, $P_{a,m}$ and $P_{a,f}$, respectively. For notation simplicity, it assumes that these two probabilities are equal, that is, $P_{a,m} = P_{a,f} = P_a$. It is worth mentioningthat the analysis can be easily extended to the case where $P_{a,m} \neq P_{a,f}$. It assumes that all sensing reports are independent. It is noted that the distribution of each sensing report is determined by the environment and the behavior`r of the corresponding sensor node. Let the sensing report of node i be $u_i \in \{0, 1\}$, where i = {1, . . . , n}. If node i is benign, then u_i is a Bernoulli random variable characterized by detection probability P_d if the target is present, or the false alarm rate P_f if the target is absent; if node i is malicious, then u_i is a Bernoulli random variable characterized by the parameter 1 - P_a if the target is present, or P_a if the target is absent.

The aggregated result at the MA is given by, $U=\sum_{i=1}^{n} u_i$.The random variable U represents the number of 1's that the access point received. To apply the q-out-of-m fusion rule, U is compared to q. If $U \geq q$, the final decision is that the target is present (i.e., decide H_1); otherwise, the final decision is that the target is absent (i.e., decide H_0). This method closed-form solution is based on the central limit theorem, where the aggregated result at the access point is approximated as a Gaussian random variable. In fact, this method has the following result.

3.2 MALICIOUS NODE DETECTION AND ADAPTIVE FUSION

This section proposes to enhance the system performance through malicious node detection, where the hostile behavior is identified and the malicious sensors are discarded from the final decision making. Furthermore, this method proposes an adaptive fusion procedure, where the fusion parameters are tuned based on the attack behavior and the percentage of the malicious sensors.

3.2.1 The Malicious Node Detection Scheme

Let I_{mal} be the set of the malicious nodes, and O_{N_s} denotes the reports of all nodes till the sensing period N_s. When the attack strategy is known, and the percentage of malicious nodes is fixed, a traditional approach to find the malicious set, I_{mal}, is to maximize the a posterior probability of I_{mal}given the observations O_{N_s}. That is, the detected malicious set $\hat{I}_{mal} = \text{argmax}_{Imal} P(I_{mal}|O_{N_s})$, where $P(I_{mal}|O_{N_s})$is the conditional probability that the malicious set is I_{mal} given all the reports O_{N_s} . However, this detection approach is difficult to be implemented since it requires searching over all possible sets of I_{mal}. In this section, this method proposes a simple malicious node detection scheme, where the sensors' decision reports are used to identify the malicious nodes and estimate their attack behavior. Let $P_{a,f}$ (i) and $P_{a,m}$(i) denote the probabilities that the i^{th} node attacks when the target is absent and present, respectively. Let $\hat{P}_{a,f}$ (i) and $\hat{P}_{a,m}$ (i) be their estimated versions. It estimates $P_{a,f}$ (i) and $P_{a,m}$(i) by using two counters for each node at the mobile access point. More specifically, for node i,

$T_{i,0}$: represents the number of times node i sends "0" when the final decision is "1". $T_{i,1}$: represents the number of times node i sends "1" when the final decision is "0". These counters are updated after each sensing period by comparing the final decision (obtained using the q-out-of-m rule) with the individual sensing reports. Assuming the observation interval is N sensing periods, and the number of observations where the access point decides that the target is present and absent are N_1 and N_0, respectively. Then, if the node is benign, $\frac{T_{i,0}}{N_1}$ and $\frac{T_{i,1}}{N_0}$ would be indications for the i^{th} node's miss detection probability and false alarm rate, respectively. On the other hand, if node i is malicious, $\frac{T_{i,0}}{N_1}$ and $\frac{T_{i,1}}{N_0}$ will be estimates for $P_{a,m}$(i) and $P_{a,f}$(i), respectively. The proposed method defines the thresholds $\lambda_{p,f}$ and $\lambda_{p,m}$ as,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

$$\lambda_{p,f} = P_f + \delta_{f,0}; \lambda_{p,m} = P_m + \delta_{m,0} \quad (2)$$

where P_f and P_m are the benign nodes' false alarm and miss detection probabilities, $\delta_{f,0}$ and $\delta_{m,0}$ represent the tolerance in the estimated false alarm rate and miss detection probability of the nodes. The malicious node detection procedure has two levels:

Level 1: Discard the suspicious reports. If $\frac{r_{i,0}}{N_1} \geq \lambda_{p,m}$ or $\frac{r_{i,1}}{N_0} \geq \lambda_{p,f}$, the node's report is discarded from the current decision process, but its counters will continue to be updated in the next sensing periods.

Level 2: Discard the unreliable nodes. If $\frac{r_{i,0}}{N_1} \geq P_m + \delta_1$ or $\frac{r_{i,1}}{N_0} \geq P_f + \delta_2$, where δ_1 and δ_2 are relatively large, then the corresponding node will be discarded from the sensing process. The nodes' counters will continue to be updated to estimate the attack probability.

3.3 ADAPTIVE FUSION ALGORITHM

Adaptive fusion can be achieved by updating the value of the q-out-of-m fusion parameters based on the average probability of attack. Recall that I_{mal} is the set of detected malicious nodes, then $|I_{mal}|$ is the total number of sensors detected to be malicious. The estimated average attack probability is given by,

$$\hat{P}_a = \frac{1}{|I_{mal}|} \sum_{i=1}^{|I_{mal}|} \hat{P}_a(I_{mal}(i)) \quad (3)$$

where $I_{mal}(i)$ is the i^{th} detected malicious sensor and $\hat{P}_a(I_{mal}(i)) = \frac{r_{I_{mal}(i),0} + r_{I_{mal}(i),1}}{N}$. Then, q is tuned using Proposition 1 with the new problem settings, where $n \leftarrow |I_{mal}| \rightarrow n$, $k \leftarrow |I_{mal}| \rightarrow k$, α = k/n and $P_a = \hat{P}_a$. This method defines η_d and η_f as the detection accuracy and false alarm rate of the malicious node detection scheme, respectively. That is,

$$\eta_d \triangleq \frac{N_{MM}}{k}; \eta_f \triangleq \frac{N_{BM}}{n-k} \quad (4)$$

where N_{MM} is the number of malicious nodes detected to be malicious, NBM is the number of benign nodes mistakenly regarded as malicious, k is the total number of malicious sensors and (n-k) is the number of benign sensors. Note that $I_{mal} = N_{MM} + N_{BM}$.

IV. RESULTS AND DISCUSSION

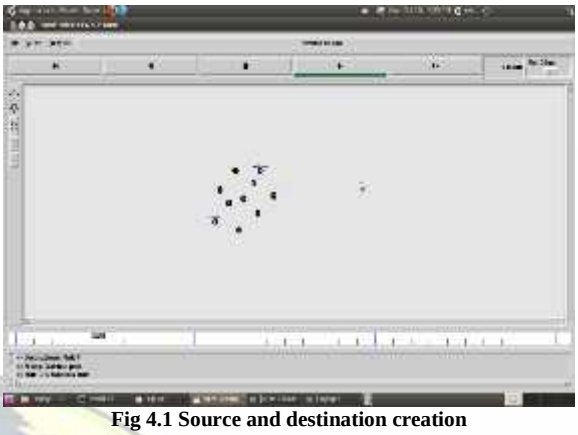

Fig 4.1 Source and destination creation

Fig 4.1 shows the source and destination creation. The network is formed with 10 nodes. Here node 0 indicates source node and node 9 indicates the destination node.

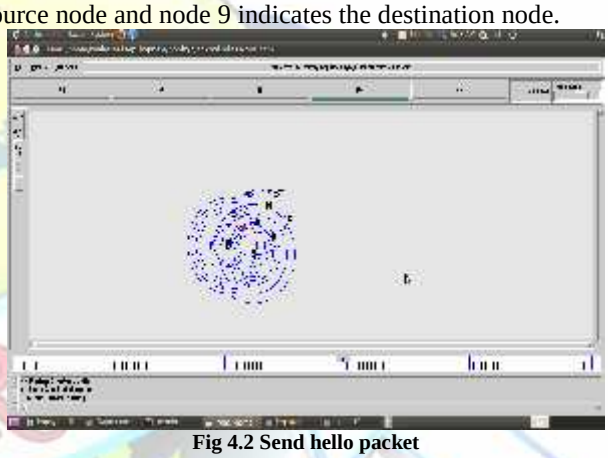

Fig 4.2 Send hello packet

Fig 4.2 shows the hello packets sending between nodes. The hello packet contains the MAC address that is each node send its address to its neighbor nodes.

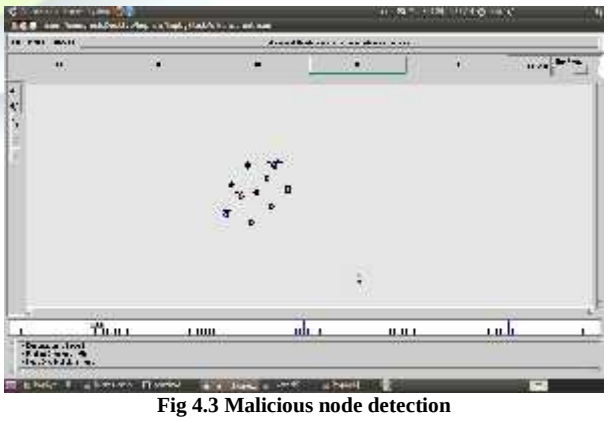

Fig 4.3 Malicious node detection

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

Fig 4.3 shows malicious node detection. The node 3 is malicious node because it does not send the packet to its neighbors. The malicious node 3 is marked as red circle.

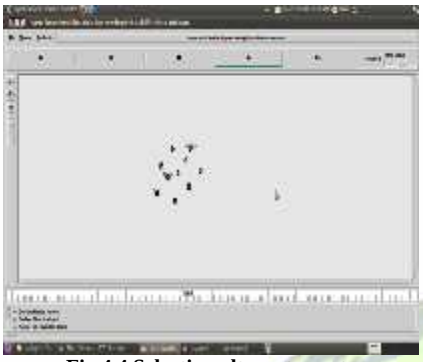

Fig 4.4 Selecting alternate route

Fig 4.4 shows selection of alternate route. The alternate shortest path is found to send the information securely.

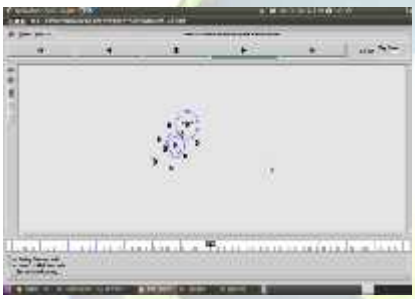

Fig 4.5alternate secure routing

Fig 4.5 shows the alternate secure routing. The information in the form of packet is send to its destination via secure routing.

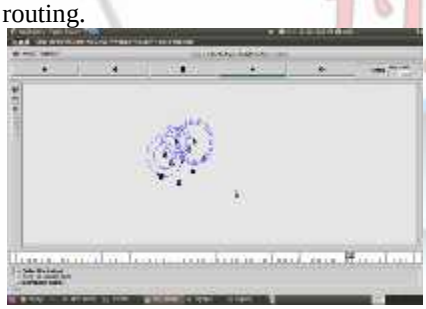

Fig 4.6 Destination send a reply data to source via same secure routing

Fig 4.6 shows the packet sending from destination to source via secure routing. The destination sends a reply message to source.

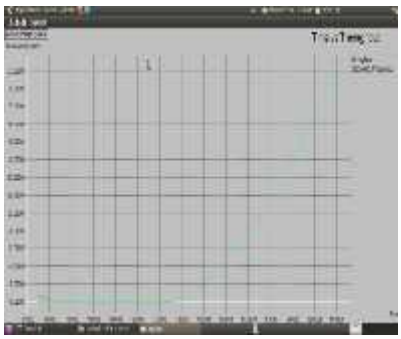

Fig 4.7 Throughput graph

Fig 4.7 shows the throughput graph. The graph is plotted between time versus throughput. At the start of simulation the throughput is decreased because of the presence of malicious node. Then after finding the alternate secure routing path the packet is securely transmitted. So, the throughput is increased after the malicious node detection.

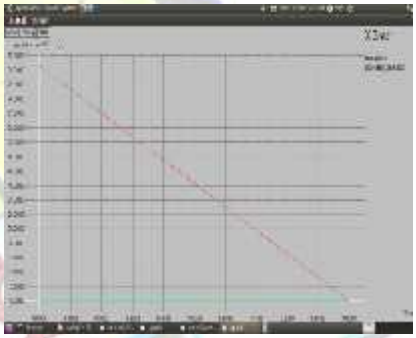

Fig 4.8 Packet loss graph

Fig 4.8 shows the packet loss graph. The graph is plotted between time versus packet loss. The graph shows the comparison of existing system packet loss and proposed system. The red color line indicates the existing system packet loss. In this the packet loss can be decreased as the time increases. The green color line indicates the packet loss of proposed system. There is no packet loss in the proposed system.

V CONCLUSION

This scheme uses the q-out-of-m fusion rule for SENMA networks under Byzantine attacks. Both static and dynamic attack strategies were discussed. It proposes simplified q-out-of-m fusion schemes by exploiting the linear relationship between the scheme parameters and the network size. It is also derived a near-optimal closed-form solution for the fusion threshold based on the central limit theorem. An important observation is that, even if the percentage of malicious sensors remains fixed, the false alarm rate diminishes exponentially with the network size. This implies that for a fixed percentage of malicious nodes,

it can improve the network performance significantly by increasing the density of the nodes.

Furthermore, it is obtained an upper bound on the percentage of malicious nodes that can be tolerated using the q-out-of-m rule. It is found that the upper bound is determined by the sensors' detection probability and the attack strategies of the malicious nodes. Finally, it proposed an effective malicious node detection scheme for adaptive data fusion under time varying attacks. The detection procedure is analyzed using the entropy-defined trust model, and has shown to be optimal from the information theory point of view. It is observed that nodes launching dynamic attacks take longer time and more complex procedures to be detected as compared to those conducting static attacks. The adaptive fusion procedure has shown to provide significant improvement in the system performance under both static and dynamic attacks.

REFERENCES

[1]. Y.-C. Wang and Y.-C. Tseng, "Distributed Deployment Schemes for Mobile Wireless Sensor Networks to Ensure Multilevel Coverage," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 9, pp. 1280-1294, Sept. 2008.

[2]. P. Barooah, H. Chenji, R. Stoleru, and T. Kalmar-Nagy, "Cut Detection in Wireless Sensor Networks," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 3, pp. 483-490, Mar. 2012.

[3]. A. Bharathidasas and V. Anand, "Sensor Networks: An Overview," technical report, Dept. of Computer Science, Univ. of California at Davis, 2002.

[4]. C. Chong and S. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," Proc. IEEE, vol. 91, no. 8, pp. 1247-2056, Aug. 2003.

[5]. A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler, "Spins: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, pp. 521-534, Sept. 2002.

[6]. C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A Link Layer Security Architecture for Wireless Sensor Networks," Proc. Second Int'l Conf. Embedded Networked Sensor Systems, pp. 162-175, http:// doi.acm.org/10.1145/1031495.1031515, 2004.

[7]. L. Lightfoot, J. Ren, and T. Li, "An Energy Efficient Link-Layer Security Protocol for Wireless Sensor Networks," Proc. IEEE Int'l Conf. Electro/Information Technology, pp. 233-238, May 2007.

[8]. I. Rodhe, C. Rohner, and A. Achtzehn, "n-lqa: n-Layers Query Authentication in Sensor Networks," Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems, pp. 1-6, Oct. 2007.

[9]. W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE 27th Conf. Computer Comm., pp. 1418-1426, Apr. 2008.

[10]. D. Martins and H. Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey," Proc. 13th Int'l Conf. Network-Based Information Systems (NBiS '10), pp. 313-320, Sept. 2010.

[11]. H. Chan, A. Perrig, and D. Song, "Secure Hierarchical in-Network Aggregation in Sensor Networks," Proc. 13th ACM Conf. Computer and Comm. Security (ACM CCS '06), pp. 278-287, 2006.

[12]. H. Kumar, D. Sarma, and A. Kar, "Security Threats in Wireless Sensor Networks," IEEE Aerospace and Electronic Systems Magazine, vol. 23, no. 6, pp. 39-45, June 2008