ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (390-403), Month: April-June 2014, Available at: www.researchpublish.com

Distributed Detection of Byzantine Attacks in WSNs: A Short Critical Survey

Mohan N[1], Akram Pasha[2]

[12]Department of Computer Science & Engineering, REVA Institute of Technology and Management,

Bangalore, INDIA

Abstract: **Wireless Sensor Networks (*WSNs*) have played a vital role, and is considered to be one of the immense and emerging technologies as there are various innovative applications both for public sector and military organizations. The type of sensing technology used in *WSN*s combined with the processing power continue to be productive and get to be utilized in abundance in the forth coming applications. Therefore, due to their unlimited prospective views, *WSN*s are currently receiving significant attention in various domains of research. Additionally, despite the fact that *WSN*s are characterized by severely constrained computational and energy resources, they are still complemented by their unlimited potential and hence they are currently getting trivial interest. However, it is still too early in the lifetime of such systems to get established, as there exist many research challenges that are yet to be met. Consequently, much research has been focused on making sensor networks feasible and useful rather than concentrating much on the security aspects of the deployment.**

Therefore, the objective of the work proposed in this article is to critically study the security aspects of *WSN*s, considering the Distributed Detection of Byzantine Attacks in particular.

Keywords: **Security in *WSN*s, Byzantine Attacks, Distributed Detection.**

I. INTRODUCTION

A Wireless Sensor Networks (WSNs)

A *WSN* is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Fig.1 shows the typical Multihop *WSN* architecture. The development of *WSN*s was originally motivated by military applications such as battlefield surveillance.

However, *WSN*s are now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control.

In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The envisaged size of a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust, although functioning 'motes' of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from hundreds of pounds to a few pence, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.

Most of the research in the field of Distributed Detection has been carried out under the assumption of a secure network. Only in the recent past, researchers have investigated the problem of security threats on sensor networks. In this paper, we shown the different methodologies used by different authors under the Byzantine attack (also referred to as the Data Falsification Attack). Byzantine attack involves malicious sensors within the network which send false information to the Fusion Center (*FC*) to disrupt the global decision making process.

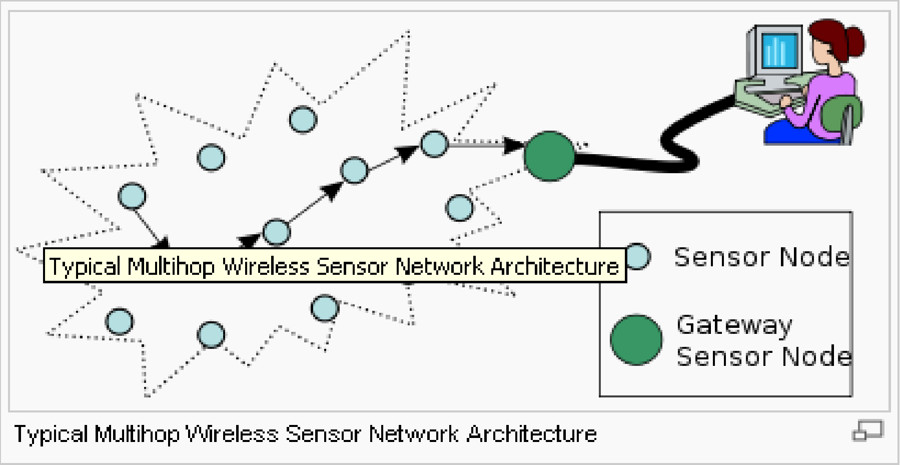
Typical Multihop Wireless Sensor Network Architecture
Sensor Node
Gateway Sensor Node
Typical Multihop Wireless Sensor Network Architecture

Fig. 1 Multihop WSN Architecture

B. Byzantine Attacks

Byzantines intend to deteriorate the detection performance of the network by suitably modifying their decisions before transmission to the *FC*. In the work proposed in [27], the Distributed Detection problem in the presence of Byzantines under the assumption that the Byzantines have perfect knowledge of the underlying true hypothesis is studied. Many studies have also presented the optimal attacking distributions for the Byzantines such that the detection error exponent is minimized at the *FC*. In this current study, we not only summarize different methods proposed in many research studies, but also propose the research challenges to improve the performance of the Distributed Detection in the presence of Byzantines.

In the effort of this study, Byzantine Attacks are not only considered to be the most severe threat to *WSN*s, but they tend to make it more challenging to protect it from gaining full control over some of the authenticated nodes, eventually, which may lead to the uninformed behavior to disrupt and collapse the system.

C. Distributed Detection

Distributed Detection is a classical subject in signal processing and has attracted recent interest due to the potential deployment of wireless sensors for a variety of applications from environmental monitoring to military surveillance. While there is a vast literature on secure networking for general ad hoc and sensor networks. And, several studies [3]–[5], have reported on Distributed Detection and data fusion in the presence of Byzantine Sensors, which is still bound by several challenges.

Therefore, the objective of the work published in this article, is to survey the role of Distributed Detection in the presence of Byzantine Attacks. The chapters of the article are organized as follows. Chapter 1 introduces the problem of Distributed Detection in *WSN*s in the presence of Byzantine Attacks. Chapter 2 discusses the significance and need for studying such a problem through elaborating the Classical problem of Distributed Detection. And, it discusses the scenario of a Byzantine Sensor with an extra power Intruder.

II. NEED FOR DISTRIBUTED DETECTION IN THE PRESENCE OF BYZANTINE ATTACKS

A. Classical Problem of Distributed Detection

The classical problem of Distributed Detection considered in the work [38], limits the sensors to get compromised by an intruder. As a result, all the compromised sensors which refer to as Byzantine tend to get reprogrammed by the intruder to attack the *FC* by transmitting fictitious observations. The uncompromised sensors that are referred to as honest can then follow the expected rule of operation. But, in the context of distributed detection, sensors are more vulnerable to tampering due to the Byzantine Sensor problem which is particularly motivated by the applications of envisioned *WSN*s. However, the wireless sensors then can be made of low cost devices adhering to the severe constraints on battery power. But, this requires that such practical limitations to make use of sophisticated encryption which eventually makes it more unrealistic.

Furthermore, the wireless transmission medium is more vulnerable to eavesdropping, which makes it possible for the attacker to extract information from sensor transmissions. As a result, the adversary can employ a wide range of strategies including deploying its own sensors aimed at jamming the transmission of honest sensors or, in a more sophisticated way, transmitting optimally designed signals to confuse the *FC*.

The analytical characterization of the ability that Byzantine Sensors can affect the decision at the *FC* is considered is further elaborated in this study [38]. Specifically, this work is proposed from the intruder's perspective, and suggests the most effective attacking strategies by the Byzantine Sensors. As a result, it is evident that when too many sensors are compromised, the *FC* will lose its ability to detect the underlying phenomenon. But this work proposed lack in defining 1. The minimum population size of the Byzantine Sensors such that the fusion network is rendered ineffective completely. 2. the achievable performance without knowing which sensor is compromised in a situation where a decision maker is bound by an upper bound or with the given sensor population.

The work proposed in [1], a standard model in Distributed Detection under binary Hypotheses *H0 versus H1* with known distributions is studied. In such a model, all the sensors are assumed to draw observations that are independent, and identically distributed (*i.i.d*) and conditioned on the unknown hypothesis. But, as studied in [2], the classical assumption of conditional independent and identically distributed (*i.i.d*) observations may not always be valid in practice and the literature is evident of such complications of correlated observations. Therefore, the work studied in [1], Recognizes the limitations, and makes the conditional independent and identically Distributed (*i.i.d*) assumption for analytical tractability and gains insights into how Byzantine Sensors can affect the overall performance.

B. Byzantine Sensor with an Extra Power Intruder

Wherever the Byzantine Sensors are used, the literature has shown that when the approach that grants the Intruder with more power than usually allowed in practice leads to the conservative assessment of security risk but with an advantage of having increased the productivity of analytical tractability. Consequently, such an assumption with a known true hypothesis leads to the utilization of the knowledge to construct the most effective fictitious observations aimed at confusing the *FC*.

Therefore, the studies have shown that such assumptions are apparently difficult to be satisfied in real world. As it would make it necessary that the attacker has a separate network that allows Byzantine Sensors to cooperate themselves.

However, within the context of the *FC*, the two important assumptions are made, 1. the Byzantine Sensors are not to get compromised. 2. The Byzantine Sensors are to be able to collect data from n sensors. But, this method lacks in giving the necessary mechanisms to make an individual sensors deliver their data to the *FC* except that what the *FC* receives is what transmitted by the sensors (Byzantine or honest). Additionally, this simplifying assumption also has practical implications: transmissions of sensors may need to be protected by error control mechanisms, and the Byzantine Sensors are not able to alter the transmissions of honest sensors. As a result, the assumption is made that any *FC* will not have any sufficient knowledge about which sensor is Byzantine.

The *FC* is empowered to know the average percentage of compromised sensors, or at least an upper bound, and that the Byzantine Sensors may create fictitious samples according to some unknown (possibly optimized) distribution. The adversary is aware that the *FC* makes the detection under a variant of Neyman-Pearson (*NP*) setup [2]. The *FC* caps the false alarm probability for all possible attacking distributions which happens to be different from the standard NP problem, not knowing what distribution the attacker adopts. It is not only difficult but impossible to minimize the miss detection probability for all possible attacking strategies. Therefore, a reasonable approach is to minimize the worst miss detection probability, which guarantees that the miss detection probability will not exceed that advertised the worst case, no matter which distribution is used by the Byzantine Sensors.

Byzantine models have also been of prime interest in the recent research work on network security. But, these models are mainly focused on the impact of Byzantine nodes on distributed detection, which is apparently new in the current research arena.

In a nut shell, the problem in the presence of compromised sensors is analogous to the original Byzantine general problem, wherein the set of sensors try to interference the *FC* to reach reliable detection, and the compromised sensors, like the traitorous general, are given full options (including collaboration) to disrupt the sensor network. However, the key difference in such a problem is the presence of the *FC* (which is always honest) itself. An information theoretic investigation of data fusion in the presence of Byzantine Sensors is studied in the work [9]. But, in this work the prime focus is in recovering measurements from honest sensors at the *FC*, not in the detection performance. Additionally, the signal processing problem studied in this method is most relevant to robust statistical inference [10].

Further, in his seminal work proposed in the work [11], the problems of binary hypothesis testing with contaminated distributions are studied. The Byzantine Sensor model used in such a method fits naturally into [10] Huber's robust detection framework, and as a result the classical robust detection problem is applied to the Byzantine Sensor problem. In particular, [10] showed that the likelihood ratio test based on the worst distribution pair has the minimax property. Because, it minimizes the maximum miss detection error probability (among all possible–contaminated distributions) while all the false alarm probabilities are below a preset bound.

These results, however, are not a direct application of those of [10]. In [11], the miss detection error exponent is used as a performance metric in the analysis. While as the work in [10] is inclined towards the worst distribution pair, the technique used in [11] consider them as different. This technique leads to a "water filling" solution whereas the technique used in [10] is algebraic.

However, finding the worst distribution pair is only the first step toward characterizing the power of the Byzantine attack. For example, in the work [11], the result shows the relation between the size of the Byzantine Sensor population and the worst detection error exponent. Additionally, the work proposed in [11] investigates the effects of multiple sensor measurements and the scaling behavior, which are not considered in classical robust detection.

III. FALSE DISCOVERY RATE-BASED DISTRIBUTED DETECTION IN THE PRESENCE OF BYZANTINES

A. Distributed Detection with Fusion of Local Decisions

It is evident from the Literature that there is an increased interest in using the *WSN*s in monitoring the region of interest (*ROI*) for reliable detection/estimation/tracking of events. In the work proposed in [16], the prime focus is on distributed target detection in *WSN*s, which is considered to be one of the very recent and active areas of research. Consequently, when the focus is on distributed detection, due to power and a bandwidth constraint, each sensor, instead of sending its raw data, sends quantized data (local decision) to a central observer or Fusion Center (*FC*). As a result, the *FC* combines these local decisions based on a fusion rule to come up with a global decision.

In the work proposed in [16], the prime focus is on Distributed Detection with fusion of local decisions. The work proposed in [13], optimum fusion rules have been derived for the Distributed Detection problem under various assumptions. Most of these fusion rules require complete knowledge of the local sensor performance metrics, such as the probability of detection and false alarm. However, in large *WSN*s and under complex target signal models, the local sensor performance metrics may not be known or may be very difficult to estimate. To address this scenario of unknown local sensor performance metrics, the work proposed in [20], suggest employing the total number of detections (also referred to as the *count statistic*) as a decision statistic at the *FC*. The fusion rule based on the count statistic leads to a decision rule where the sensor decisions are weighed equally, even though the *SNR* at each sensor may be different.

B. False Discovery Rate

In general, the work proposed in [16] says that obtaining the optimal local decision rules is very difficult problem. Under the conditional independence assumption, the work proposed in [14], has been shown that the use of identical local decision rules is optimal under asymptotic conditions (i.e., the number of sensors N → ∞). Although the optimality of identical decision rules does not hold in general [17] [18], design of non-identical decision rules is computationally very complex and researchers have generally employed identical decision rules based on asymptotic optimality of identical decision rules. However, the studies [15], [11] have proposed the False Discovery Rate (*FDR*) based distributed detection.

The work [15][11], proposed a scheme for Distributed Detection in *WSN*s based on the control of *FDR*. It has been shown that under the assumption that the *FC* employs a test statistic which is linear in count (count here refers to the total number of detections) to reach the global decision, control of the *FDR* leads to non-identical local decision rules and provides significant improvement over the system with identical decision rules. This scheme provides significant improvement in the global detection performance.

However, this study suggests the maximization of the deflection coefficient to obtain the *FDR* design parameter. But, the maximization of the deflection coefficient does not guarantee optimal global performance. Further, in this study [15], the problem of *FDR* based Distributed Detection is considered, and it is shown through demonstration that system performance can be improved by optimizing the *Kolmogorov-Smirnov* distance instead of the deflection coefficient. The key contributions of the study made in [15] are as summarized below:

•Maximization of the *Kolmogorov-Smirnov* distance instead of the deflection coefficient to obtain the *FDR* design parameter and demonstrate that it considerably improves system performance.

• A byzantine attack model is defined and shown that the *FDR* value is controlled even in the presence of Byzantines; however the local sensor detection performance deteriorates considerably when the fraction of Byzantines is large.

• The performance of *FDR* based Distributed Detection in the presence of Byzantine Attacks is studied and provide the analytical and simulation results on the effect of Byzantines on global detection performance.

• Finally, an algorithm which adaptively changes the system parameters by learning the Byzantines' behavior over time is proposed and demonstrated that the proposed algorithm provides improved system performance in the presence of Byzantines.

- The implications and some implementation issues are also discussed.

The study conducted in this work is followed from the work proposed in [48] and is observed that deflection coefficient is not the best heuristic for the design of *FDR* based Distributed Detection framework in non-asymptotic cases. Hence, they explored other possible distance measures that can better serve as design heuristics. Through empirical studies and analytical justifications, shows the system performance can be improved by the use of *Kolmogorov-Smirnov* distance as the design heuristic. The advantage of using distance measures is the simplicity associated with its implementation in practice. The optimization is performed offline by finding the optimal parameter value through brute-force search. For a large number of sensors, it can also use the asymptotic expressions which can be computed in linear time. Also, the distributed algorithm used in this framework reduces the energy and bandwidth consumption since the local sensors only report their 1-bit decisions to the *FC*.

C. Strategy of Byzantine Attack

In the work proposed in [16], the system in the presence of malicious sensors (Byzantines) is studied and modeled the Byzantines' attack strategy to ensure covertness in its behavior (since *FDR* value is still controlled at the pre-determined threshold), while degrading the system performance in terms of detection probability. It is also observed that the optimal parameter value for the system primarily depends on the fraction of Byzantines present in the system. The system performance degrades under severe attacks when fixed parameter values are used and, therefore, this study proposed an adaptive approach to improve the performance, which would eventually degrade the presence of Byzantines. However, in this work, because the sensors are deployed in a dynamically changing environment, an adaptive scheme is necessary to combat the adversaries in the network. The proposed scheme under this study learns the fraction of Byzantines present in the network and adaptively changes system parameter values to improve the global detection performance.

The survey conducted lists several research directions in this domain in the chapter entitled "Conclusion and Future Research Challenges".

IV. BYZANTINE SENSORS IN DISTRIBUTED SOURCE CODING

A. Distributed Source Coding Problem

In the work proposed in [39], authors consider a modification to the distributed source coding problem in which an unknown subset of sensors are taken over by a malicious intruder and reprogrammed. Considering that there are *m* sensors. Each time slot, sensors *i for i= 1….,m* observe random variables according to the joint probability distribution *P(X1….,Xm).* Each sensor encodes its observation independently and transmits a message to a common decoder, which attempts to reconstruct the source values with small probability of error based on those messages. A subset of sensors are considered as *traitors*, while the rest are considered as *honest*. Apart from the honest sensors or the decoder, the traitors have been reprogrammed to cooperate to obstruct the goal of the network, launching a so-called Byzantine Attack. To counter this attack, the honest sensors and decoder must employ strategies so that the decoder can correctly reconstruct source values no matter what the traitors do. Therefore, the authors observe that it is quite obvious that the observations made by the traitors are irretrievable unless the traitors choose to deliver them to the decoder. And the best decoder can hope to achieve is to reconstruct the observations of the honest sensors. Further, the authors give a simple procedure that is to ignore the statistical correlations among the observations and then collect data from each sensor individually. The total sum rate of such an approach is given by *Ei H(Xi).* One expects however that this sum rate can be lowered if the correlation structure is not ignored.

B. Slepian–Wolf Coding

Without traitors, *Slepian–Wolf* coding [20] can be used to achieve a sum rate as low as *H(X1….Xm).* But the standard Slepian–Wolf coding has no mechanism for handling any deviations from the agreed-upon encoding functions by the sensors. Even a random fault by a single sensor could have devastating consequences for the accuracy of the source estimates produced at the decoder, to say nothing of a Byzantine Attack on multiple sensors. In particular, because *Slepian–Wolf* coding takes advantage of the correlation among sources, manipulating the codeword for one source can alter the accuracy of the decoder's estimate for other sources. It will turn out that for most source distributions, the sum rate cannot be achieved if there is even a single traitor.

C. Example of Distributed Inference Problem

The work proposed in [39], overcomes the disadvantage of Slepian-Wolf coding and shows the interest in the lowest achievable sum rate such that the decoder can reconstruct observations of the honest sensors with arbitrarily small error probability. In some cases, the author further shows an interest in the rate region. Although the problem setup does not allow the detector to distinguish traitors from the honest sensors, an efficient scheme that guarantees the reconstruction of data from honest sensors is of both theoretical and practical interest. Therefore, the example of distributed inference problem in the presence of Byzantine Sensors is studied. For such a problem a practical (though not necessarily optimal) solution is to attack the problem in two separate phases. In the first phase, the decoder collects data from sensors over multiple access channels with rate constraints. Here it requires that the data from honest sensors are perfectly reconstructed at the decoder even though the decoder does not know which piece of data is from an honest sensor. In the second step, the received data is used for statistical inference. The decoder may also have other side information about the content of the messages that allows the decoder to distinguish messages from the honest sensors.

V. DISTRIBUTED INFERENCE IN THE PRESENCE OF BYZANTINE SENSORS

A. Byzantines

A large Wireless Sensor Network (*WSN*) engaged in the task of distributed binary detection is considered in the work proposed in [43]. The network consists of *n* nodes or sensors, each making an independent and identically distributed (*iid*) observation about the State of the Nature (say *H1* or *H0*). These observations are successively delivered to a common *FC* for the final decision on the underlying statistical hypothesis. In point of fact the network is under attack: a clique of traitorous sensors cooperatively works against the network. These sensors, referred to as the Byzantines (and the kind of attack described is then called Byzantine Attack [27]), deliver data according to certain fictitious distributions properly designed in order to impair the detection capability of the *FC*. The Byzantines are assumed to know the true underlying hypothesis; the uninfected and *FC*. The *FC*, however, is aware of the presence of the Byzantines. Specifically, it knows that a fraction of the sensors are traitorous and will deliver data drawn according to the optimal (from the Byzantine viewpoint) attacking distributions. Consequently, the decision rule implemented at the *FC* is a Neyman-Pearson test that do account for the fraction of fictitious data. The strategy described in this work is more sophisticated than the naivest black hole attack, in which the intruder simply destroys the owned fraction of sensors. In this scenario, a network is referred implicitly in which each node makes a single observation about the State of the Nature by considering network in which *m* individual sensors form a cluster, and there are *n* different clusters. Wherein, either all the *m* sensors of a cluster are Byzantine or all are honest, and the sensors become clusters of sensors, with each cluster delivering to the *FC* a vector of m samples.

B. Network Design

Two system architectures are possible to be designed for a sensor network involved in Distributed Detection under a Byzantine Attack: 1. a network made of individual sensors, and 2. a hierarchical structure with groups of m sensors tied together to form a cluster. For the former architecture, this study has shown that if more than 50% of the nodes are Byzantine, the attack can always destroy any detection capability by making a network useless. Therefore, in this work, the fundamental tradeoff between detection capability and attacking power is characterized, the optimal attacking probability laws are derived, and finally the decision rule implemented at the *FC* is used to be a censored likelihood ratio test. This test bears similarities to Huber's robust statistics. Whereas, in the clustered network, this analogy breaks down and different behaviors arise. As a result, the attackers owning less than one half of the total sensors cannot completely impair the system. They can, however, severely degrade the performance of the network, and the optimal attacking distributions that achieve this goal are "hypothesis-reversed": the Byzantine emissions are drawn from the distribution corresponding to the false State of the Nature.

A remarkable fact that was observed in this work is that the asymptotic detection probability does not scale exponentially with the cluster size. In fact, it does not scale at all with m. And, eventually, the practical consequence occurred is a saturation effect. In other words, it is observed that increasing the number of per-cluster sensors beyond a certain amount does not provide any significant performance improvement. On the other hand, the expected scaling law is instead preserved with respect to the total number of clusters.

VI. SENSOR NETWORKS WITH MOBILE AGENTS

A. What are SENMAs?

A *SENMA* is new network architecture for low power and large scale sensor networks. *SENMA* stands for Sensor Networks with Mobile Agents (*SENMA*). *SENMA* have two types of nodes: sensors and mobile agents. Sensors in *SENMA* are low power and low cost nodes that have limited processing and communication capability. The battery operated sensors have a finite operational life and low duty cycles. And deployed in a large quantity instead randomly through aerial drop and it is impossible and no need to have a careful network layout.

B. Significance of Adding Mobile Agents to SENMA

Mobile Agents [29] are not considered to be software programs that migrate from host to host in the network, rather, they are powerful hardware units, both in their communication and processing capability and in their ability to traverse the

Sensor Network. The work proposed in [29] the examples of Mobile Agents that are manned/unmanned aerial vehicles; ground vehicles equipped with sophisticated terminals and power generators, or specially designed light nodes that can hop around in the network are considered. These Mobile Agents may have high data rate connections to satellites, allowing reach back to remote command control centers. It is been observed that the Mobile Agents need not always have to be present or be operational along with sensors in *SENMA*, instead, they could be in actions only when it is necessary to collect the data and perform network maintenance.

VII. BYZANTINE ATTACKS IN DISTRIBUTED DETECTION IN *WSN*S

A. Sensors Deployment and Uses

The facilities of sensors deployment and the cost reductions have become the two major reasons to see the increase in utilizing the uses of *WSN*s. Until recently, this kind of networks are found useful in industrial monitoring, environmental data record, home automation , fire detection , medical or even in military applications, and so on and so forth. But, most of these applications are deployed to monitor an area and to have a reaction when they record a critical factor. However, it is evident from the literature that the data need not be confidential in the areas such as home automation or the capture of environmental events. But confidentiality of data becomes of utmost pertinent in other applications, such as for medical diagnostic of a patient in a hospital or for the security of a territory in military. Therefore, the solutions that are used in conventional ad hoc networks cannot be applied in *WSN*s, because the sensors are limited by their battery and computing power. Specifically, cryptographic solutions currently used such as public key cryptography are not adapted to be calculated by unpowerful processors of current sensors. Additionally, this imposes many restrictions. One such restriction asks us to have all security protocols to limit the number of messages needed for its proper functioning, because communication between sensors is the main source of energy consumption in *WSN*s

B. Byzantine Attack in SENMA

The work proposed in [42] studies the problem of distribute detection, by assuming that the serious threat to *WSN*s is the Byzantine Attack (See Fig. 2). Further, this work observes that given some solutions to overcome from this type of attacks, the adversary has full control over some of the authenticated nodes and can perform arbitrary behavior to disrupt and collapse the system completely. Therefore, this study further extends its work by considering the reliable data fusion in *WSN*s with mobile access points [34] under both static and dynamic Byzantine Attacks. In such a scenario, the malicious nodes report false information with a fixed or time-varying probability.

The major contributions of the work proposed in [42] are summarized as below:

First, a simplified, linear *q out- of-m* scheme that can be easily applied to large size networks is proposed. The basic idea in such a scheme is to find the optimal scheme parameters at relatively small network sizes through exhaustive search, and then to obtain the fusion parameters for large network size by exploiting the approximately linear relationship between the scheme parameters and the network size. Eventually, it is observed that this newly proposed linear approach can achieve satisfying accuracy with low false alarm rate. However, this scheme is still inherent to some issues, which may violate the problem constraint. Therefore, to enforce the miss detection constraint and improve the data fusion accuracy, this work extends the discussion and propose to use the linear approximation as the initial point for the optimal exhaustive search algorithm.

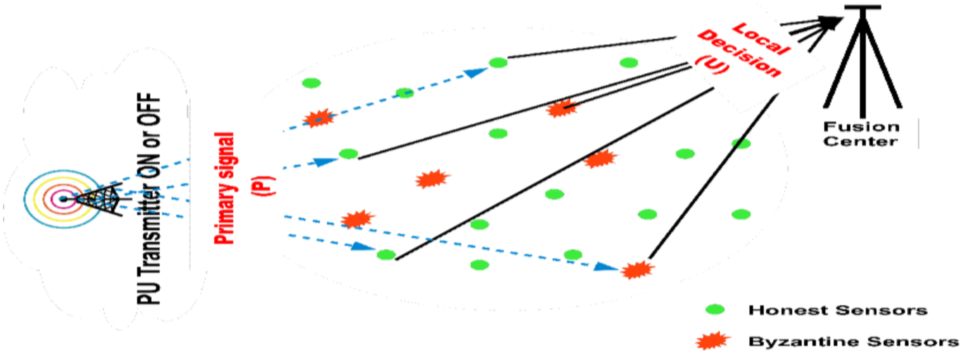

Fig. 2 WSN Architecture under Byzantine Attacks

With this enhanced linear approach, they obtained near-optimal solutions with much lower computational complexity compared with that of the pure exhaustive search approach.

Second, in an effort to search for an easier and more flexible distributed data fusion solutions and which can easily adapt to unpredictable environmental changes, and cognitive behavior of malicious nodes. They also derived a closed-form solution for the *q-out-of-m* fusion scheme based on the central limit theorem. And 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 is shown here that the closed-form solution delivers comparable results with that of the near-optimal solution obtained from the enhanced linear approach.

Third, they perform some theoretical analysis for both the linear approach and the closed-form solution. It shows that under a fixed percentage of malicious nodes, the false alarm rate for both approaches diminishes exponentially as the network size increases. This analysis reveals an interesting and important result: even if the percentage of malicious nodes remains unchanged, larger size networks are much more reliable under malicious attacks. This indicates that the network size plays a critical role in reliable data fusion. Moreover, the upper bound on the percentage of malicious nodes that can be tolerated by the network under the q-out-of-m fusion rule is found. It turns out that this upper bound is determined by the sensors detection probability and the attack strategies of the malicious nodes.

Finally, they come up with 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 *FC*. And their observations shows that dynamic attacks generally take longer time and more complex procedures to be detected as compared to static attacks. They also found that their proposed malicious detection procedure can identify malicious sensors accurately if sufficient observation time is allowed. This proposed approach is analyzed again using an entropy-based trust model. And show that under the same system settings, the proposed malicious node detection approach is optimal from the information theory point of view. Further propose a method to adapt the fusion parameters based on the detected malicious sensors and their estimated probability of attack. It is shown that the newly proposed adaptive fusion scheme can improve the system performance significantly under both static and dynamic attack strategies.

VIII. CONCLUSION AND FUTURE RESEARCH CHALLENGES

In this study, primarily the need for Distributed Detection in the presence of Byzantine Attacks is discussed. Further, to understand the essence of Distributed Detection in the presence of Byzantine Attacks, the classical problem of Distributed Detection is elaborated. Subsequently, the scenario of a Byzantine Sensor with an extra power Intruder is discussed to explore the various configurations of such a problem. Further, to comprehend the setting of Distributed Detection under such attacks, the false discovery rate based Distributed Detection in the presence of Byzantines is elaborated. Distributed Source Coding in the Presence of Byzantine Sensors and Distributed Inference in the Presence of Byzantine Sensors are also discussed to understand the significance of Distributed source coding and inference in the presence of Byzantine Sensors. Finally, although the study conducted is not exhaustive, the sensor networks with Mobile Agents are also discussed to complete the discussion.

The work done in this study not only provides the critical appraisal in the area of Distributed Detection of *WSN*s in the presence of Byzantine Attacks, but also lists the various research challenges in such a domain.

A. Byzantine Attacks in Distributed Detection in Mobile Access WSNs

In the work proposed in [42], the q-out-of-m fusion rule for *SENMA* networks under Byzantine Attacks is studied by considering both static and dynamic attack strategies. In this work, simplified q-out of-m fusion schemes are proposed by exploiting the linear relationship between the scheme parameters and the network size by also deriving a near-optimal closed-form solution for the fusion threshold based on the central limit theorem. An important observation in such a scheme 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, there is still a room for further research and can improvement of the network performance significantly by increasing the density of the nodes. Therefore, the future research challenges could be to conduct an adaptive detection under Byzantine Attacks by considering soft decision reports.

B. Byzantine Attacks in Distributed Detection (in general)

In the work proposed in [38], Distributed Detection in the presence of Byzantine Sensors created by an intruder is studied. Further, this work characterizes the power of attack analytically. As a result, this work is able to provide closed-form expressions for the worst detection error exponent of an optimized NP detector at the *FC*, and for the corresponding attacking distributions. The work further gives an expression of the minimum attacking power above which the ability to detect is completely destroyed. As to the case of vector observations, they find that an intruder infecting less than 50% of the nodes cannot completely impair the system, regardless of the distributions of the sensors' observations.

Therefore, there are number of future research challenges:

1. It may be of interest to consider a Bayesian formulation with *a priori* probabilities assigned to the hypotheses, so that the asymptotic performance can be measured in terms of the *Chernoff* information [44] in such a setting.

2. The tools and schemes that were used in this work can be further exploitable for studying the attacks of a less dangerous intruder that does *not* know the true state of the nature.

C. Byzantines in False Discovery Rate-based (FDR) Distributed Detection

In the work proposed in [48], the problem of *FDR* based Distributed Detection in the presence of Byzantines is discussed. Firstly, it studies the work proposed in [38] and is observes that deflection coefficient is not the best heuristic for the design of *FDR* based Distributed Detection framework in non-asymptotic cases. Hence, in this work, there are several observations made:

1. It is shown that there are several other possible distance measures that can better serve as design heuristics are explored.

2. Through empirical studies and analytical justifications, it is observed that system performance can be improved by the use of *Kolmogorov-Smirnov* distance as the design heuristic. The advantage of using such distance measures is the simplicity associated with its implementation in practice.

3. It is observed that the optimization is performed offline by finding the optimal parameter value through brute-force search.

Further, this work explores the system in the presence of malicious sensors (Byzantines). Subsequently, it models the Byzantines attack strategy to ensure covertness in its behavior (since *FDR* value is still controlled at the pre-determined threshold) while degrading the system performance in terms of detection probability. And, the system performance is analyzed both theoretically and numerically. Eventually, the two important observations are made; 1. The optimal parameter value for the system depends on the fraction of Byzantines present in the system. 2. The system performance degrades under severe attacks when fixed parameter values are used. Based on these observations, this work proposes an adaptive approach to improve the performance which degraded in the presence of Byzantines. Correspondingly, the sensors are deployed in a dynamically changing environment and, therefore, an adaptive scheme is considered to be necessary to combat the adversaries in the network. This scheme not only learns the fraction of Byzantines present in the network but also adaptively changes system parameter values to improve the global detection performance.

The following are the several directions for future work on this problem.

1. One could explore other distance measures such as proposed in [49] that can be used as heuristics for system design.

2. The optimal attack strategy for the Byzantines needs to be derived as it would be interesting to see how the performance of the network depends on the optimal attack strategy of the Byzantines defined by **h***opt(.)*, wherein, the *Neyman-Pearson* framework is considered. This work could be further extended to a Bayesian framework where the problem is to detect the presence of a random target. For this, one may need to employ the Bayesian version of *FDR* called Bayesian *FDR* [50] or p*FDR* [51]. In the work proposed in [50], an approach for control of Bayesian *FDR* has been proposed which can be used to design local sensor thresholds in Distributed Detection under the Bayesian framework similar to the work in [48] and the present work.

D. Byzantine Sensors in Distributed Source Coding

In the work proposed in [9], an explicit characterization of the region of achievable rates for a Byzantine attack on distributed source coding with variable-rate codes, deterministic fixed-rate codes, and randomized fixed-rate codes are dealt. Correspondingly, it was observed that a different set of rates were achievable for all the above the three cases mentioned earlier, and therefore, the converse proofs and rate achieving coding schemes for each were given. Further, it also elaborates that the variable-rate achievability could be shown by using an algorithm in which sensors use randomness to make it unlikely that the traitors can fool the coding process.

Therefore, there is still much of the future research to be done in the area of Byzantine network source coding. Additionally, in this work, multi-terminal rate distortion such as used in the works [45], [46] could be further studied, or other topologies, such as side information could be further explored. However, the inherent tradeoff in this work is that because the traitors cannot in general be identified, it is difficult to imagine applications that do not require some post processing of the source estimates. Thus it would be of interest to take up the future research to solve the coding and estimation problems simultaneously, as is shown in the CEO problem discussed in [47].

E. Byzantine Sensors in Variable-rate Distributed Source Coding

In the work proposed in [57], the Variable-Rate Distributed Source Coding in the Presence of Byzantine Sensors is studied assuming that the traitors have access to all the source values. However, such an assumption is considered to be vital in many of the converse proofs that are dealt in this work. But, this is a significant assumption that may not be all that realistic. Therefore, it would be worthwhile, though perhaps it appears to be more difficult, to perform the following in the future research line.

1. Firstly, to characterize the achievable rate region without this assumption.

2. Secondly, performing the variable-rate source coding by assuming that the traitors have access only to their own source values or possibly degraded versions of those of the honest sensors.

Finally, considering the Byzantine Attacks on other sorts of multi-terminal source coding problems, such as the rate distortion problem shown in the works [52], [53] or the CEO problem [54] still remains as the future research challenge.

F. Byzantine Sensors in Distributed Inference

In the two described system architectures [43] addresses the following basic questions. What are the optimal attacking distributions that the Byzantine will employ? What is the resulting test performance? What about the minimum fraction of traitorous sensors/clusters such that the network becomes useless? A related information theoretical view of Byzantine Attacks in WSNs is provided in [28], where the focus is on the capacity of collaborative fusion. The presence of misinformed nodes is instead dealt with in [29].

G. Byzantine Attacks in Collaborative Spectrum Sensing (Cognitive Radio Networks (CRN))

In the work proposed in [35], several fundamental issues related to collaborative spectrum sensing for *CRN*s in the presence of Byzantine attackers is considered. However, this work is an extension of the work proposed in [55] to the realistic scenario in distributed data fusion, where the true state of nature is expected to be unknown. To experiment further, the performance limits boundaries have been established to create independent and cooperative Byzantine Attacks. This work further elaborates the optimal strategies for the Byzantines and the *FC* by using the *minimax* approach. But, there are still many interesting research questions that are yet to be explored in the future work. The first research question asks us to analyze the dynamic interaction among the Byzantines and the *FC* to find the optimal strategies which can maximize their performance in finite cycles of data fusion. The second research question could be to perform the similar analysis, but, by considering the case where Byzantines collude in several groups to increase their objective to degrade the detection process.

H. Mobile Agents in Sensor Networks

Finally, the work proposed in [56], provides architecture for large low power sensor network for *SENMA*. However, apart from several features, the key feature of *SENMA* is the addition of Mobile Agents that shifts processing complexities away from sensors. As a result, SENMA offers considerable advantage in energy efficiency over the Rat ad hoc network architecture. This work also proposes a joint design of Physical *MAC* layer that leverages advantages of Mobile Agents and exploits the inherent node redundancies. However, this work is not exhaustive in exploring all the design options at different levels of the protocol stack. Therefore, exploring a wide range of design options at different levels of the protocol stack for *SENMA* and for specific applications still remain as the research challenge in this domain.

ACKNOWLEDGEMENT

The authors would like to thank the management, Faculty and Staff of Department of Computer Science & Engineering, REVA Institute of Technology, who have helped directly and indirectly, to make this work successful.

REFERENCES

[1] J. N. Tsitsiklis, “Decentralized detection,” in *Advances in Signal Processing*, H. V. Poor and J. B. Thomas, Eds. New York: JAI Press, 1993, pp. 297–344.

[2] P. Willett, P. Swaszek, and R. Blum, “The good, bad and ugly: Distributed Detection of a known signal in dependent Gaussian noise,” *IEEE Trans. Signal Process.*, vol. 48, pp. 3266–3279, Dec. 2000.

[3] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route filtering of injected false data in sensor networks,” *IEEE J. Sel. Areas Commun.*, vol. 23, pp. 839–850, Apr. 2005.

[4] X. Luo, M. Dong, and Y. Huang, “On distributed fault-tolerant detection in wireless sensor networks,” *IEEE Trans. Comput.*, vol. 55, pp. 58–70, Jan. 2006.

[5] T. Clouqueur,K. K. Saluja, and P. Ramanathan, “Fault tolerance in collaborative sensor networks for target detection,” *IEEE Trans. Comput.*, vol. 53, pp. 320–333, Mar. 2004.

[6] L. Lamport, R. Shostak, and M. Pease, “The Byzantine generals problem,” *ACM Trans. Program. Languages Syst.*, vol. 4, pp. 382–401, Jul. 1982.

[7] D. Dolev, “The Byzantine generals strike again,” *J. Algorithms*, vol. 3, no. 1, pp. 14–30, 1982.

[8] B. Pfitzmann and M.Waidner, “Information Theoretic Pseudosignatures and Byzantine Agreement. 1996, IBM Research Report,Tech. Rep. RZ2882.

[9] O. Kosut and L. Tong, “Distributed source coding with Byzantine sensors,” *IEEE Trans. Inf. Theory*, vol. 54, 2008.

[10] S. A. Kassam and H. V. Poor, “Robust techniques for signal processing: A survey,” *Proc. IEEE*, vol. 73, pp. 433–481, Mar. 1985.

[11] P. J. Huber, “A robust version of the probability ratio test,” *Ann. Math. Statist.*, vol. 36, no. 6, pp. 1753–1758, Dec. 1965.

[12] P. K. Varshney, *Distributed Detection and Data Fusion*. New York: Springer, 1997.

[13] Z. Chair and P. Varshney, “Optimal data fusion in multiple sensor detection systems,” *IEEE Trans Aerosp. Electron. Sys.*, vol. 22, pp. 98–101, Jan. 1986.

[14] R. Viswanathan and P. Varshney, “Distributed detection with multiple sensors: Part I — Fundamentals,” *Proc. IEEE*, vol. 85, no. 1, Jan. 1997.

[15] J. Tsitsiklis, “Decentralized detection,” in *Advances in Statistical Signal Processing*, H. Poor and J. Thomas, Eds. Greenwich, CT: JAI Press, 1993.

[16] R. Niu, P. Varshney, and Q. Cheng, “Distributed Detection in a Large Wireless Sensor Network,” *International Journal on Information Fusion*, vol. 7, no. 4, pp. 380–394, Dec. 2006.

[17] J. Tsitsiklis, "Decentralized Detection by a large number of sensors," *Mathematics of Control, Signals, and Systems (MCSS)*, vol. 1, pp. 167–182, 1988.

[18] E. Ermis and V. Saligrama, "Distributed detection in sensor networks with limited range multimodal sensors," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 843 –858, Feb. 2010.

[19] P. Ray and P. K. Varshney, "Distributed detection in wireless sensor networks using dynamic sensor thresholds," *International Journal of Distributed Sensor Networks*, vol. 4, no. 1, pp. 5–12, 2008.

[20] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. IT-19, pp. 471–480, 1973.

[21] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Tra. Program. Lang. Syst.*, vol. 4, pp. 382–401, Jul. 1982.

[22] T. Ho, B. Leong, R. Koetter, M. Médard, M. Effrons, and D. Karger, "Byzantine modification detection in multicast networks using randomized network coding," in *IEEE Proc. Intl. Symp. Inf. Theory*, Jun.- Jul. 27–2, 2004, p. 143.

[23] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An on-demand secure routing protocol resilient to Byzantine failures," in *ACM Workshop Wireless Security (WiSe)*, Sep. 2002.

[24] O. Kosut and L. Tong, "Capacity of cooperative fusion in the presence of Byzantine sensors," in *Proc. 44th Annu. Allerton Conf. Commun., Contr. Comput.*, Monticello, IL, Sep. 27–29, 2006.

[25] T. H. S. Jaggi, M. Langberg, and M. Effros, "Correction of adversarial errors in networks," in *Proc. Int. Symp. Inf. Theory Applicat.*, Adelaide, Australia, 2005.

[26] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, pp. 382-401, July 1982.

[27] O. Kosut and L. Tong, "Capacity of cooperative fusion in the presence of Byzantine sensors," in Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, September 27-29 2006.

[28] Z. Yang and L. Tong, "Cooperative sensor networks with misinformed nodes," IEEE Trans. Inform. Theory, vol. IT-51, no. 12, pp. 4118-4133, Dec. 2005.

[29] D. Kotz and R. S. Gray, "Mobile agents and the future of the internet:' *IEEE Trans. Automr. Contc*, vol. AC-28, pp. 1081-1090, December 1983.

[30] E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, and A. Chandrakasan, "Physical Layer Driven Protocol and Algorithm Design for Energy-Efficient Wireless Sensor Networks," in *Proc. of 2001 ACM MOBICOM*, (Rome, Italy). pp. 272-286, July 2001.

[31] K. Sohrabi, B. Manriquez, and G. Pottie, "Near Ground Wideband Channel Measurement," in *Proc. of the 49th Vehicular Technology Conference*, (Houston), pp. 571-574, May 1999.

[32] G. Pottie and W. Kaiser, "Wireless Integrated Network Sensors," *Communications of the ACM*, vol. 43, pp. 5 1-58. May 2000.

[33] T. Rappaport, "*Wireless Communications Principles and Practice"* Prentice Hall, 1996.

[34] G. Mergen, Z. Qing, and L. Tong, "Sensor networks with mobile access: Energy and capacity considerations," *IEEE Transactions on Communications*, vol. 54, no. 11, pp. 2033 –2044, Nov. 2006.

[35] A.Rawat, P. Anand, H. Chen, and P. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *Signal Processing, IEEE Transactions on*, vol. 59, no. 2, pp. 774 –786, Feb. 2011.

[36] R. Viswanathan and V. Aalo, "On counting rules in distributed detection," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 37, no. 5, pp. 772 –775, May 1989.

[37] R. Niu and P. Varshney, "Performance analysis of distributed detection in a random sensor field," *IEEE Transactions on Signal Processing*, vol. 56, no. 1, pp. 339 –349, Jan. 2008.

[38] Stefano Marano, Vincenzo Matta, and Lang Tong, *IEEE "*Distributed Detection in the Presence of Byzantine Attacks" *IEEE Transactions On Signal Processing*, Vol. 57, No. 1, January 2009.

[39] Oliver Kosut and Lang Tong*,”* Distributed Source Coding in the Presence of Byzantine Sensors” *IEEE Transactions On Information Theory*, VOL. 54, NO. 6, JUNE 2008

[40] L. Tong, Q. Zhao, and S. Adireddy, “Sensor networks with mobile agents” *IEEE Military Communications Conference, MILCOM 2003*, vol. 1, pp. 688 – 693, Oct. 2003.

[41] M. Abdelhakim, L. Lightfoot, and T. Li, “Reliable data fusion in wireless sensor networks under Byzantine Attacks,” *IEEE Military Communications Conference, MILCOM 2011*, Nov. 2013.

[42] Mai Abdelhakim, Leonard E. Lightfoot, Jian Ren, and Tongtong Li *“Distributed Detection in Mobile Access Wireless Sensor Networks Under Byzantine Attacks”* Digital Object Indentifier 10.1109/TPDS.2013.74.

[43] Stefano Marano, Vincenzo MattaLang Tong *“Distributed Inference in the Presence of Byzantine Sensors”.*

[44] T. Cover and J. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[45] S. Y. Tung, “Multiterminal Source Coding,” PhD, Cornell University, Ithaca, NY, 1978.

[46] T. Berger, *The Information Theory Approach to Communications*, G. Longo, Ed. Berlin, Germany: Springer-Verlag, 1978, Chapter Multiterminal source coding.

[47] T. Berger, Z. Zhang, and H. Viswanathan, “The CEO problem [multiterminal source coding],” *IEEE Trans. Inf. Theory*, vol. 42, pp. 887–902, May 1996.

[48] P. Ray and P. K. Varshney, “False Discovery Rate based sensor decision rules for the Network-wide distributed detection problem,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 47, no. 3, pp. 1785 –1799, 2011.

[49] M. Basseville, “Distance measures for signal processing and pattern recognition signal processing,” *Signal Processing*, vol. 18, no. 4, pp. 349–369, 1989.

[50] A. S. Whittemore, “A Bayesian False Discovery Rate for multiple testing,” *Journal of Applied Statistics*, vol. 34, no. 1, pp. 1–9, 2007.

[51] J. D. Storey., “The Positive False Discovery Rate: A Bayesian interpretation and the q value,” *The Annals of Statistics*, vol. 31, no. 6, pp. 2013–2035, 2003.

[52] S. Y. Tung, Multiterminal Source Coding. PhD thesis, Cornell University, Ithaca, NY, 1978.

[53] T. Berger, The Information Theory Approach to Communications (G. Longo, ed.), chapter Multi-terminal source coding. Springer-Verlag, 1978.

[54] T. Berger, Z. Zhang, and H. Viswanathan, "The CEO problem [multiterminal source coding]," IEEE Trans. Inform. Theory, vol. 42, pp. 887- 902, May. 1996.

[55] S. Marano, V. Matta, and L. Tong, “Distributed detection in the presence of byzantine attack in large wireless sensor networks,” in *Military Communications Conference, IEEE MILCOM 2006*, Oct. 2006, pp. 1–4.

[56] Oliver Kosut and Lang Tong, *“Variable-Rate Distributed Source Coding in the Presence of Byzantine Sensors”* ISIT2007, Nice, France, June 24 - June 29, 2007.

[57] Lang Tong, *Qing* Zhao, and Srihari Adireddy “Sensor Networks with Mobile Agents” IEEE 0-7803-814WO3S17.W 2003.

Author(s) Profile:

Mohan N, received Bachelor of Computer Science Engineering from Visvesvaraya Technological University, Belgaum, Karnataka. He is now pursuing Master of Technology in Computer Network Engineering. His research interests are developing the security mechanisms for WSNs.

Akram Pasha, Associate Professor, Department of Computer Science and Engineering, Reva Institute of Technology and Management, Bangalore, India.