ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Distributed Detection in Mobile Access Wireless Sensor Networks UnderByzantine Attacks

A.D.K.Nirmala
M.Tech Student,
Department of CSE,
Aditya Engineering College.

T.Sudha Rani
Sr. Asst. Professor,
Department of CSE,
Aditya Engineering College.

ABSTRACT:

In Adhoc network the Byzantine Attack is the most safety threads as it bring to a halt in the communication of nodes in the network and behave like a fair nodes while take part normally in the network. It is very important in the network to provide the communication between the nodes is to be error free and communication takes place in a particular time period. In a tree based topology every node is take part in communication with other nodes.

So it is major challenge to protect the data transmission between the nodes in the network as many types of attacks are collaborating with Byzantine attack. In order to provide optimal strategy to generate the attack in the network and also provide the good way to attack the precious node which will affect the network with a big loss. some solution is to be provided so the attack can be take place on the most important node who have the confidential data in it, with the cost associated to the node and some algorithm should provide in order to find the time delays between the nodes also provide bounds to the nodes in order to transmit the data.

detect the faulty data transmission and also limits the use of the resources by falling the investment of resources which takes part in communication.we propose an effective malicious node detection scheme for adaptive data fusion under time-varying attacks; the proposed scheme is analyzed using the entropy-based trust model, and shown to be optimal from the information theory point of view. Simulation examples are provided to illustrate the performance of proposed approaches under both static and dynamic attacks.

Keywords:

Security in wireless sensor networks, Byzantine attacks, Distributed detection.

INTRODUCTION:

In Adhoc network the data transmission process is required to capture the sending packets from one source to other destination so as to mean to provide cost to every node in the network the security to the packets in order to deal with the communication specially in the tree based network where every nodes participate in communication .

As the data transmission takes place many other malicious nodes involves in the communication process and behaves like a fair nodes and always take part in communication while sending the faulty data to the other nodes and make the whole network faulty. There are many attack are generated in the network as the communication takes place between the nodes. It is very difficult to detect the malicious nodes from the whole network.

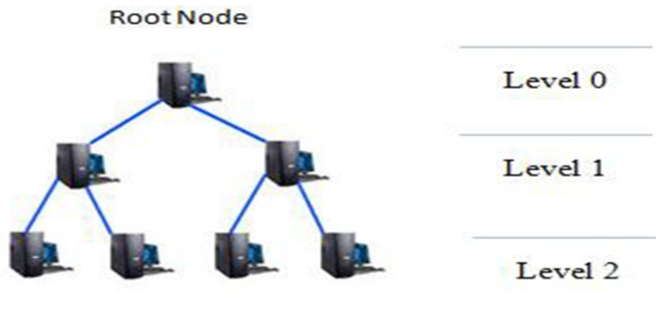
In tree network the data can be distributed so that at the particular need of the data they should be available so the communication takes place smoothly but in that same condition many attacks are generated and in the case of Byzantine attack many attacks are automatically combine with it. So the main focus on this paper is to detect the attack on the network which combines with Byzantine attack and also the Byzantine attack is the most dangerous attack as it compromises the nodes in the network and behaves like a normal on.

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.

It will overcome with the distributed environment while the data available to the nodes when it demands, while the data load on the network may decrease, resources always available for the data transmission, automatically time delays from that particular reason may also decrease, also increase the transmission area of the nodes and maintain hierarchy into the tree while levels associated to it.



Hierarchy of Tree Topology

BYZANTINE ATTACK:

Byzantine attack is the most promising attack in which it compromises the nodes and the set of the compromise nodes are able to take part in communication while behaving like a normal nodes and make a communication strong but with a falsified packet delivery also associated with it. So the detection t such attack is very difficult also time consumption may take place. Major challenge in the detection of Byzantine attack is that many other attack are also deployed with it so the work of detection also increases as the network increase therefore in some distributed detection scheme should introduce in order to deal with the situation.

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 WSNs, 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.

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, have reported on Distributed Detection and data fusion in the presence of Byzantine Sensors, which is still bound by several challenges.
It is simple to implement, and can achieve a good tradeoff between minimizing the miss detection probability and the false alarm rate. In ideal scenarios, the optimal scheme parameters for the q-out-of-m fusion scheme are obtained through exhaustive search. However, due to its high computational complexity, the optimal q-out-of-m scheme is infeasible as the network size increases and/or the attack behavior changes.

To overcome this limitation, effective sub-optimal schemes with low computational complexity are highly desired. The main contributions of the paper can be summarized as follows: First, we propose a simplified, linear q-out- of-m scheme that can be easily applied to large size networks.

The basic idea is to find the optimal scheme parameters at relatively small network sizes through exhaustive search, and then obtain the fusion parameters for large network size by exploiting the approximately linear relationship between the scheme parameters and the network size. It is observed that the proposed linear approach can achieve satisfying accuracy with low false
alarm rate.

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. It indicates that the network size plays a critical role in reliable data fusion. Moreover, we also find an upper bound on the percentage of malicious nodes that can be tolerated by the network under the q-out-of-m fusion rule. It turns out that this upper bound is determined by the sensors‘ detection probability and the attack strategies of the malicious nodes.

Finally, we propose 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. It is also found that the proposed malicious detection procedure can identify malicious sensors accurately if sufficient observation time is allowed.

The proposed approach is analyzed using an entropy-based trust model. We show that under the same system settings, the proposed malicious node detection approach is optimal from the information theory point of view. We further propose to adapt the fusion parameters based on the detected malicious sensors and their estimated probability of attack. It is shown that the proposed adaptive fusion scheme can improve the system performance significantly under both static and dynamic attack strategies.

System Overview:

The network is composed of n power-limited sensor nodes and a powerful mobile access point. We assume that the nodes are randomly and uniformly distributed over the network, and the mobile access point traverses the network on a predefined trajectory to communicate with all the sensing nodes. The sensor network performs distributed detection. Each sensor node detects the presence of the target object by applying an application dependent detection algorithm, such as energy detection, and sends its one-bit hard decision report to the mobile access point (1‘ means that the target is present),which makes the final decision accordingly.

This hard decision model is adopted here for two reason: (1) To reduce the transmission and processing burden of the sensor network; (2) To enable more tractable analysis on the effect of the network size on the reliability of the distributed detection under Byzantine attacks. The network covers a large area, we divide the area into smaller sections, and apply the fusion rule over nodes that are within the same section. This setting ensures that, statistically, nodes within the same section have the same chance of detecting the target.

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 WSNs in monitoring the region of interest (ROI) for reliable detection/estimation/tracking of events. The prime focus is on distributed target detection in WSNs, 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.

B.False Discovery Rate:

In general, the work proposed in says that obtaining the optimal local decision rules is very difficult problem. Under the conditional independence assumption, the work proposed, 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 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 have proposed the False Discovery Rate (FDR) based distributed detection.

C. Strategy of Byzantine Attack:

In the work proposed, 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.

Modeling of Possible Attack Strategies:

There are different attack strategies that could be adopted by the malicious sensors. Let Po be the probability that each malicious node intentionally reports the opposite information to its actual sensing decision. It is assumed that all malicious nodes have the same probability of attack in a particular sensing period. We classify the possible attack strategies into two categories:

1) Static Attack: In this strategy, the malicious nodes send opposite data with an arbitrary probability Po that is fixed, with 0 < Po ≤ 1.

2) Dynamic Attack: In this strategy, the malicious nodes change Po after each attacking block, which is composed of one or more sensing periods.

Simplified Data Fusion Scheme – The Linear Approach
To develop effective sub-optimal schemes with low computational complexity, it is important to know how the parameters m and q change with the system variables, such as α and n. In this section, we consider the case where the malicious sensors attack with probability Pa.

We calculate the optimal parameters at different Pa values, under different network sizes and different percentages of malicious sensors. 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 we can get the optimal scheme parameters at relatively small network sizes, and use them as reference points.

Malicious Node Detection and Adaptive Fusion:

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. Further more, an adaptive fusion procedure, where the fusion parameters are tuned based on the attack behavior and the percentage of the malicious sensors.

Attack Implementation:

The respective attacks are implementing in this paper in order to detect the malicious nodes and also to avoid the incorrect packet transmission.

Blackhole attack:

In a Blackhole attack, the attacker attracts the data packets and then sends them by distributing incorrect routing information. The attacker notifies that it has an finest route. So, other normal nodes demand to route data packets through the malicious node.

Wormhole attack:

Wormhole attack is one of the most difficult forms of routing attacks. In this attack, an attacker proceedings packets at one location, tunnels them to another location of the network, where it is retransmitted by a existing attacke.

Grayhole attack:

In Grayhole attack a node can control from behaving correctly like a black hole that is it truly an attacker and it will proceed as a normal node.

Analysis:

1. Analyzing Byzantine attack in tree based network and consequences.

2. Simulating Byzantine attack using Adhoc on demand distance vector routing protocol.

3. Comparing the performance of network parameter by means of packet delivery ratio, data rating, throughput, time delays.

Discussion:

Performance can be measure with the network parameter as:

1. Packet delivery fraction: The ratio of the data packets elated to the destinations to those generated by the constant bit rate (CBR) sources is known as Packet Delivery Fraction (PDF).

2. End-to-End Delay: End-to-End delay is all possible delays due to buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times of data packets.

3. Energy Consumption: Before the transmission of data takes place each and every nodes have to be charged with some amount of energy in order to take part in communication process.Analyse the energy consumption of each nodes after the transmission. Adaptive Fusion: Closed-Form Solution with Malicious Node Detection .

The overall false alarm rate averaged over observation periods when Nth = 100. The results are further averaged over iterations to get more accurate results. It can be seen that significant performance improvement is achieved for both static and dynamic attacks when the adaptive fusion with malicious node detection is employed. The miss detection constraint is satisfied for all cases. The non-smoothness of the curves is mainly due to the tuning of the integer valued scheme parameters to satisfy the miss detection constraint. It should be noted that the thresholds δo,f,δo,m have a direct impact of the performance of the malicious node detection scheme and they could be further optimized to improve the performance.

The effect of the observation interval N on the detection accuracy of the malicious node detection scheme (ηd). It can be seen that malicious nodes launching dynamic attack require longer observation interval to be detected than nodes adopting static attack. Demonstrates that the proposed malicious node detection scheme is efficient and highly accurate. The false alarm rate of the malicious node detection scheme (ηf) is plotted versus the observation interval. As expected, it is shown that ηF decreases as more observations are available at the access point. The effect of the observation threshold Nth on ηfis illustrated in Section X of the supplementary file.

SENSOR NETWORKS WITH MOBILE AGENTS :

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:

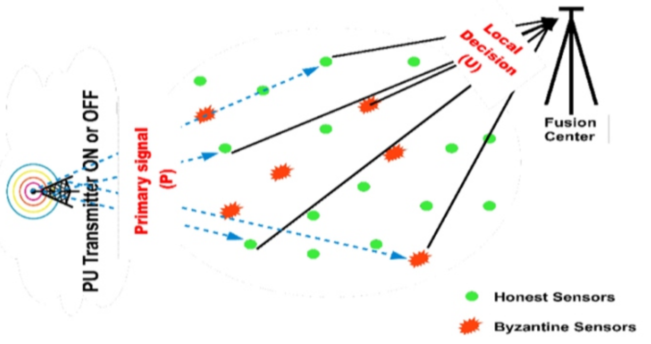
Mobile Agents are not considered to be software programs that migrate from host to host in the network, rather, they are powerful hardware units, both in their communication and processing capability and in their ability to traverse the Sensor Network.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

BYZANTINE ATTACKS IN DISTRIBUTED DETECTION IN WSNS

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 WSNs. 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.

B. Byzantine Attack in SENMA The work proposed in studies the problem of distribute detection, by assuming that the serious threat to WSNs is the Byzantine Attack. 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 WSNs with mobile access points under both static and dynamic Byzantine Attacks. In such a scenario, the malicious nodes report false information with a fixed or time-varying probability.



Conclusion:

The malicious no de 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 informationtheory point of view. It is observed that nodes launching dynamic attacks take longer time and more complexprocedures 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. Further research can be conducted on adaptive detection under Byzantine attacks with soft decision reports.

REFERENCES:

[1] Xiang He, AylinYener." Strong Secrecy and Reliable Byzantine Detection in the Presence of an Untrusted Relay," IEEE transaction on information theory, vol. 59, no. 1, January 2013.

[2] BhavyaKailkhura ,Swastik Brahma, Pramod K.Varshney,"Optimal Byzantine Attacks on Distributed Detection in Tree based Topology,"International Conference on Computing, Networking and Communication,Workshop Cyber Physical system,2013.

[3] Xiaofan He, Huaiyu Dai, PengNing," A Byzantine Attack Defender: the Conditional Frequency Check," 2012 IEEE International Symposium on Information. Theory Proceedings.

[4] ShabirSofi, Eshan Malik, Rayees Baba, Hilal Baba, Roohie Mir," Analysis of Byzantine Attacks in Adhoc Networks and Their Mitigation, ICCIT 2012.

[5] X. He and A. Yener, The Gaussian many-to-one interference channel with confidential messages,"IEEETrans. Inf. Theory, vol.57, no.5,pp. 2730–2745, May 2011.

[6] VaibhavPandit, Jung Hyun Jun and Dharma P.Agrawal,"Inherent Security Benefits of Analog Network Coding for the Detection of Byzantine Attacks in Multi-Hop Wireless Networks," 2011 Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems.

[7] MinJi Kim, Lu´isa Lima, Fang Zhao, Jo˜aoBarros,MurielM´edard, Ralf Koetter, Ton Kalker, Keesook J. Han," On Counteracting Byzantine Attacks in Network Coded.

[8] R. Koetter and F. Kschischang, "Coding for errors and erasures in random network coding," IEEE Trans. Inf. Theory, vol. 54, pp. 3579–3591, 2008..

[9] S. Jaggi, M. Lang berg, S. Katti, T. Ho, D. Katabi, and M. M´edard, Resilient network coding in the presence of byzantine adversaries in Proceedings of IEEE INFOCOM, March 2007, pp. 616 – 624.

[10] B. Awerbuch, R. Curtmola, D. Holmer, et. al," Mitigating byzantine attacks in ad hoc wireless networks,". Department of Computer Science, Johns Hopkins University, Technical Report Version 1, March 2004.