International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), Volume 5, Special Issue 2, May 2015)
International Conference on Advances in Computer and Communication Engineering (ACCE-2015)

A Survey on Malicious Node Detection in Mobile Access WSN under Byzantine Attacks

Dinesh K. R[1], Kavitha Bai[2], A. Rosline Mary[3]
[1]*PG Scholor, Dept. of CSE, Vemana IT, Bengaluru – 34.*
[2,3]Asst. Professor, *Dept. of CSE, Vemana IT, Bengaluru – 34*
[1]d.r.211990@gmail.com, [2]kavithabai.pawar@gmail.com, [3]rosy.prabu@gmail.com

***Abstract*—In Mobile Access Wireless Sensor Networks, Detecting the Malicious nodes and explores the positive data fusion under Byzantine attacks. The linear q-out-of-m rule, which is more efficient in distributed detection and can achieve a good result between the miss detection probability and the inconvenient alarm rate. The rule in which the mobile access point randomly polls reports from m sensors, however a major limitation with it is that the optimal scheme parameters can only be obtained, making it infeasible for big networks. But first, by exploiting the linear relationship between the scheme parameters and the network size, proposed a simple but effective sub-optimal linear approach. Second, for better performance and expansion, derived a near-optimal closed-form solution. Third, subjecting to a miss detection constraint, proved that the false alarm rate of q-out-of-m diminishes exponentially as the network size grows, even if the percentage of malicious nodes remains fixed.**

***Index Terms*— Malicious node, Byzantine attacks, Distributed detection, False alarm rate**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are homogeneous or heterogeneous systems consist of many small devices, called sensor nodes, that monitoring different environments as shown in the Fig.1. i.e. sensor nodes cooperate to each other and compose their local data to reach a global view of the operational environment; they also can operate autonomously. In WSNs there are two other components, called "aggregation points" (i.e. cluster-heads and CIDSs' deployment locations) and "base stations" (i.e. central server and the WSNIDS's deployment location), which have more powerful resources and capabilities than normal sensor nodes. Aggregation points collect information from their nearby sensors, integrate and aggregate them and then forward to the base stations to process gathered data.

Factors such as wireless, unsafe, unprotected and shared nature of communication channel, untrusted and broadcast transmission media, deployment in hostile and open environments, automated and unattended nature and limited resources, make WSNs vulnerable and susceptible to many types of attacks [1].The reliable data fusion in wireless Sensor Networks with Mobile Access points (SENMA). In SENMA, the Mobile Access point (MA) traverses the network and collects the sensing information from the individual sensor nodes. The major advantage of the SENMA architecture is that it ensures a line of sight path to the access point within the power range of the sensor nodes, allowing the information to be conveyed without routing. This feature makes it a resilient, scalable and energy efficient architecture for wireless sensor networks. In many cases, due to bandwidth and energy limitations, the sensors quantize their sensing result into a single bit. The MA receives the sensing reports and applies the fusion rule to make the final decision. One popular hard fusion rule used in distributed detection is the q-out-of-m scheme [16], in which the mobile access point randomly polls reports from m sensors, then decides that the target is present only if q or more out of the m polled sensors report '1'. 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 over-come this limitation, effective sub-optimal schemes with low computational complexity are highly desired.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), Volume 5, Special Issue 2, May 2015)
International Conference on Advances in Computer and Communication Engineering (ACCE-2015)

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 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. However, there are chances of violating the problem constraint. To enforce the miss detection constraint and improve the data fusion accuracy, we further propose to use the linear approximation as the initial point for the optimal exhaustive search algorithm. With this enhanced linear approach, near optimal solutions can be obtained with much lower computational complexity.

In an effort to search for an easier and more flexible distributed data fusion solutions that can easily adapt to unpredictable environmental changes and cognitive behavior of malicious nodes, we derive 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. We show that the closed-form solution delivers comparable results with that of the near-optimal solution obtained from the enhanced linear approach.

II. System Model

A WSN 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 System architecture. The development of *WSN*s was originally motivated by military applications such as battlefield surveillance etc. the system architecture consists Wireless ad-hoc network and attack prevention system, the wireless ad-hoc network consists of two or more sensor nodes and attack prevention system consists of wireless Sensor Networks with Mobile Access points.

A. Sensor Detection

When sensor is used to the sensors quantize their sensing result into a single bit. The sensor sends the sensing reports and applies the fusion rule to make the final decision.

One popular hard fusion rule used in distributed detection is the q-out-of-m scheme.

B. Byzantine Attacks

Byzantines intend to deteriorate the detection performance of the network by suitably modifying their decisions before transmission to the FC. 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. There are different attack strategies that could be adopted by the malicious sensors.

Static attack: In this strategy, the malicious nodes send opposite data with an arbitrary probability P_o that is fixed, with $0 < P_o$ "1".

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

C. Mobile Access point

The MA traverses the network and collects the sensing information from the individual sensor nodes. The MA uses the binary reports of the sensor nodes to make the final decision on whether the target is present or absent. This distributed detection problem can be modeled using the conventional binary hypothesis test, where the hypothesis H_0 represents the absence of the target, and the hypothesis H_1 represents the presence of the target.

D. Polling

The end user collects information of the sensing nodes. Polling is used to collect the n no of user sensing information to MA. When MA can analysis to calculate the polling value and fix which trust and which or untrusted node. It is observed that the proposed linear approach can achieve satisfying accuracy with low false alarm rate. However, there are chances of violating the problem constraint. To enforce the miss detection constraint and improve the data fusion accuracy, we further propose to use the linear approximation as the initial point for the optimal exhaustive search algorithm.

E. Cluster Head

There is a Cluster-Head (CH) per each cluster of sensor nodes which it coverts its radio range nodes shown in Fig.1.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), Volume 5, Special Issue 2, May 2015)
International Conference on Advances in Computer and Communication Engineering (ACCE-2015)

So, the malicious node detection process does by cluster heads. If any malicious nodes are detected it reports to the base station and the base station raises the alarm to the end-user. The end-user monitors the environmental details and again sends the request to the cluster head.

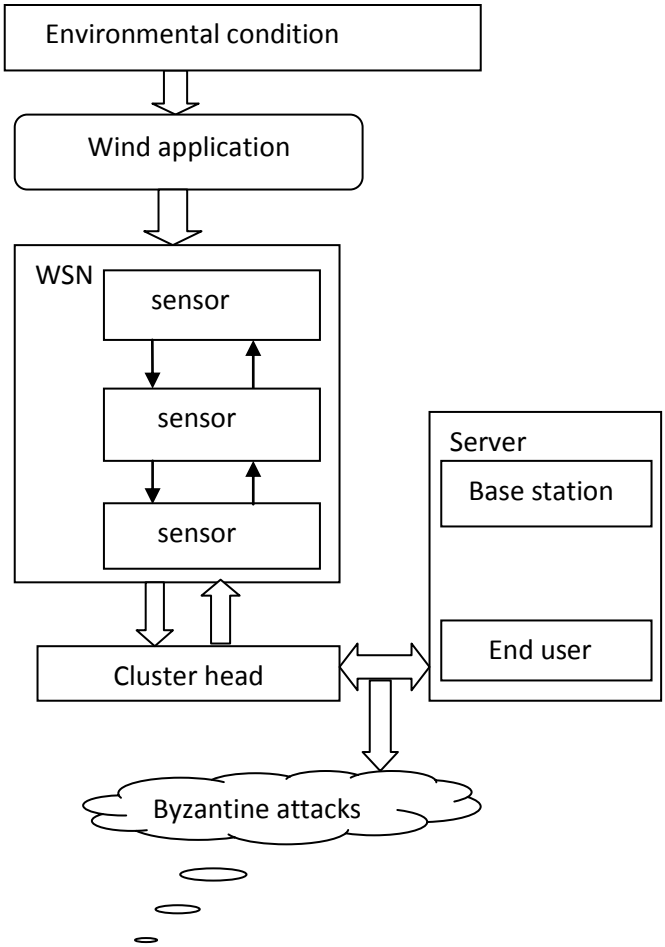

Fig. 1. System architecture

III. The Malicious Nodes

The malicious nodes which misbehaves in the wireless sensor network. It means aberration from regular routing and forwarding behavior resulting in detrimental effects on the network performance. Misbehavior arises for several reasons.

When a node is faulty its erratic behavior can deviate from the protocol and thus produces non intentional misbehavior. Intentional misbehavior aims at providing an advantage for the misbehaved node. In the wireless sensor networks.

The lack of infrastructure and organizational environment of wireless sensor networks offer special opportunities to intentionally misbehaved nodes. Without proper countermeasures, it is possible to gain various advantages by malicious behavior: better service than cooperating nodes, monetary benefits by exploiting incentive measures or trading confidential information; saving power by selfish behavior, preventing someone else from getting proper service, extracting data to get confidential information, and so on. Even if the misbehavior is not intentional, as in the case of a faulty node, the effects can be detrimental to the performance of a network.

IV. Malicious Node Activities

The malicious node activities are data dropping, modification, and misbehavior as follows:

Data Dropping: In the dropping attack, an evil node could drop all the packets it is supposed to forward or destined to it. It could also be partial dropping, which is restricted to specific types, e.g. data packets or routing packets containing Route Error. The primary interest for evil nodes is to drop data packet since dropping data packet can have more serious consequence than dropping routing packets in general. The purpose of the routing protocol is to enable the data packets exchange between any communication ends in the network.

Modification: Existing routing protocols assume that nodes do not alter the protocol fields of messages passed among nodes. Malicious nodes can easily cause traffic subversion and Denial of Service (DoS) by simply altering these fields: such attacks compromise the integrity of routing computations. By modifying routing information an attacker can cause network traffic to be dropped, redirected to a different destination or take a longer route to the destination increasing communication delays.

Misbehavior: In the wireless sensor network, some nodes misbehaves it means the nodes unable to communicate with the other nodes in network and not transmitting the exact result to the communicating node, and altering the original result means modifying the result etc..

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), Volume 5, Special Issue 2, May 2015)
International Conference on Advances in Computer and Communication Engineering (ACCE-2015)

Malicious node detection Algorithm

In the Nth sensing period, where N is sensing period index, do:
for i from 1 to n
if decision of node i is not equal to the final q-out-of-m
check if node i reports '0' and the final decision is '1'
increment Ti,o
otherwise check if node i report '1' and the final decision is'0'
increment Ti,1
end if
end if
if Ti,o
N = Pm + d or Ti,1
N = Pf + d
discard the reports of node i, and hence m is decremented
end if
end for
if the number of discarded nodes = 30%
don't discard any reports. i.e. keep m = n, but save Ti,1 and Ti,o ?i
end

V. 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.

The problem of Distributed Detection is 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.

VI. Byzantine Attacks

Byzantines diminishes the detection performance of the network by suitably modifying their decisions before transmission to the *FC*. The distributed detection problem in the presence of Byzantines under the assumption that the Byzantines have perfect knowledge of the underlying true hypothesis. 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.

The problem of distribute detection, by assuming that the serious threat to *WSN*s 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 *WSN*s 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.

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.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), Volume 5, Special Issue 2, May 2015)
International Conference on Advances in Computer and Communication Engineering (ACCE-2015)

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.

VII. False Discovery Rate

The area of multiple hypotheses tests has been an active area of research in the statistics community for several decades. Various error metrics such as the Family-Wise Error Rate (FWER) and more recently the False Discovery Rate (FDR) [10] have been proposed in this context. For the problem at hand, having an identical decision threshold for each sensor is equivalent to a strict control on the FWER. However, the control of FDR, as discussed in detail in the subsequent sections, leads to a signal dependent decision region for each local sensor. This is the primary motivation for us to propose the control of the FDR instead of the FWER to determine the local decision thresholds. We demonstrate that under the condition, that the fusion center employs a test statistic which is linear in count" to reach the global decision, control of the FDR can lead to a 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 provides 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.

VIII. Conclusion

A simplified q-out-of-m fusion rule schemes by exploiting the linear relationship between the scheme parameters and the network size, reduced the number of malicious sensors. An important observation is that, even if the percentage of malicious sensors remains fixed, the false alarm rate diminishes exponentially with the network size. It implies that for a fixed percentage of malicious nodes, can improve the network performance significantly by increasing the density of the nodes. Furthermore, the percentage of malicious nodes that can be tolerated using the q-out-of-m rule.

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] A. Rawat, P. Anand, H. Chen, and P. Varshney,"Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks," IEEE Trans. Signal Processing, vol. 59, no. 2, pp. 774-786, Feb. 2011.

[3] 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

[4] S. Marano, V. Matta, and L. Tong, "Distributed Detection in the Presence of Byzantine Attack in Large Wireless Sensor Networks," Proc. IEEE Military Comm. Conf., pp. 1-4, Oct. 2006.

[5] 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.

[6] M.R. Fellows, F.V. Fomin, D. Lokshtanov, F. Rosamond, S.Saurabh, and Y. Villanger, "Local Search: Is Brute-Force Avoidable?" J. Computer and System Sciences, vol. 78, no. 3, pp. 707-719, May 2012.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] A. S. Whittemore, ―A Bayesian False Discovery Rate for multiple testing,‖ Journal of Applied Statistics, vol. 34, no. 1, pp. 1–9, 2007.

[14] Y.L. Sun, W. Yu, Z. Han, and K. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006.

[15] A. Ghasemi and E. Sousa, "Collaborative Spectrum Sensing for Opportunistic Access in Fading Environments," Proc. First IEEE Int'l Symp. New Frontiers in Dynamic Spectrum Access Networks, pp. 131-136, 2005.

[16] L. Tong, Q. Zhao, and S. Adireddy, "Sensor Networks with Mobile Agents," Proc. IEEE Military Comm. Conf., vol. 1, pp. 688-693, Oct. 2003.