Effective Malicious Node Detection and Data Fusion under Byzantine Attacks.

ShrutiB.Hiregoudar, Manjunath K
BasaveshwarEngg College, BasaveshwarEngg College
Bagalkot ,KarnatakaBagalkot ,Karnataka

Abstract
Distributed systems are subject to a variety of failures and attacks. Many Web services are expected to run with high degree of security and dependability. As we all know that in wireless sensor network security is a major concern for protected communication between mobile nodes in a hostile environment. A serious threat to wireless sensor networks is the Byzantine attack , where the adversary has full control over some of the authenticated nodes and can perform arbitrary behavior to disrupt the system, were the attacker forwards packets through non –optimal paths or selectively dropping packets which results in disruption or degradation of routing services within the network. This paper explores effective malicious node detection and data fusion under byzantine attack by using distributed detection and checking probability condition in byzantine environment. The architecture consists of group of sensor nodes which will be sending data, a mobile access point which will periodically collect the data from sensor nodes and a sink which is used to store data sent by sensor nodes. Basically there are two types of attackers, static attracter and dynamic attracter. Static attacker, who always sends false data to sink & reverse information whenever data is requested. Dynamic attacker is attacker who sends both valid information and invalid information to sink. Hence the system gets confused weather it is a valid sensor or invalid sensor. Finally, we propose how malicious node can be detected and send only the valid data to fusion centre under byzantine attack.

Keywords: Sensor networks, distributed detection, Byzantine attack.

I. INTRODUCTION

A Wireless sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it. Sensor nodes are densely deployed in environment they are limited in power, computational capacities and memory. They transmit the information mutually, and collaboratively complete the specific function through self-organization's wireless communication. Wireless sensor network are intelligent private network which had received significant attention from the research community due to their impact on both military and civilian applications [1]. As the network go on developing security became a challenging issue presented in [2], most used detection method is distributed detection, . A Distributed detection is a well studied topicin detection theory [3]. The design of sensor networks for differentapplications has been extensively studied in the past decade. Recently, the problem of distributeddetection in the presence of Byzantine attacks has attracted attention[4],[5].The Byzantine behavior is defined as any arbitrary action by an authenticated node that results in disruption or degradation of the routing service and such an adversary is called a Byzantine adversary [6] or in otherworld's the byzantine attack is a compromised with set of intermediate, orintermediate nodes that working alone within network carry out attacks such as creating routing loops ,forwarding packets through non–optimal paths or selectively dropping packets which results in disruption or degradation of routing services within the network[7]. In this paper, we consider data fusion in wireless sensor networks with mobile access points under both static and dynamic Byzantine attacks, in which the malicious nodes report false information with a fixed or time-varying probability, respectively. Were mobile access point receives the report from sensor nodes and applies the fusion rule. One popular hard fusion rule used in distributed detection is the q-out-of-m scheme, 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'.

II. SYSTEM ANALYSIS

A. Existing System: There is centralized sensor network architecture in existing system, known as SENMA.we assume that the network is composed of n power-limited sensor nodes and a powerful mobile access point. This node are randomly and uniformly distributed over the network, and the mobile access point traverses the network to communicate with all the sensing nodes. The sensor network performs distributed detection. Each node detects the presence of the target object by applying an application dependent detection algorithm, and sends 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: To reduce the transmission and processing burden of the sensor network; To enable more tractable analysis on the effect of the

network size on the reliability of the distributed detection under Byzantine attacks. The disadvantage of existing system are :

- No Scalable and Efficiency in wireless sensor network.
- It's not suitable for large size of area.

B. Proposed System: In this paper we used flexible distributed data fusion solutions that can easily adapt to unpredictable environmental changes and cognitive behavior of malicious nodes and based on predication we will find what type of attack it is wheatear it is static attacker or dynamic attacker under byzantine attack. The following advantages are:

- Can be easily applied to large size networks.
- 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.
- Scalable and Efficiency in wireless sensor network for large size of networks. Below figure illustrate architecture of proposed model.

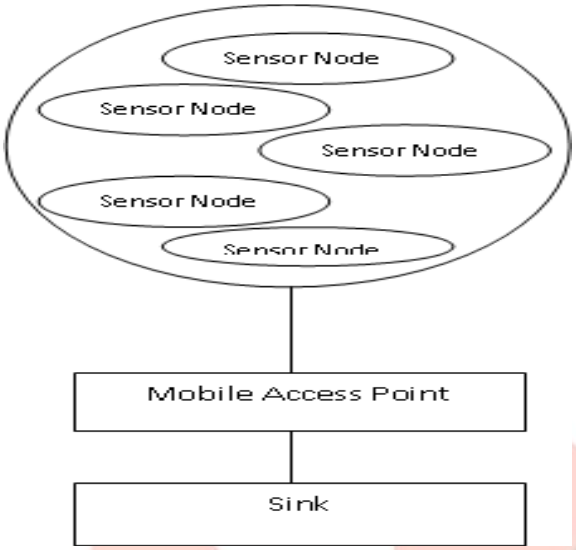

Fig 1: Architecture of proposed model

III. IMPLEMENTATION MODULES

- Sensor node
  - Normal
  - Static Attacker
  - Dynamic Attacker
- Mobile Access Point(MAP)
  - Distributed detection request
  - Data collection
  - Forward data to sink
- Sink
  - Aggregated Data Collection

At the initial level DFD represents connection of sensor nodes with the mobile access point. The sensor nodes send the ip and port no to MAP which can be further used to get data from sensor nodes. At the second stage, the MAP sends request to check the data availability with sensor nodes. When the sensor nodes get the request, they send a 0(ZERO) or 1(ONE) as reply. 1 indicates that data is available, 0 represents data is unavailable. By reading these values, MAP uses distributed detection technique to check whether the sensor nodes are normal or byzantine attackers. In third stage DFD represents data transfer from sensor nodes to sink through mobile access point. The MAP filters static attackers and dynamic attackers using distributed detection technique, then collects data from valid sensor nodes and forwards aggregated data to sink. When data is received by sink, it separates each message and displays to user.

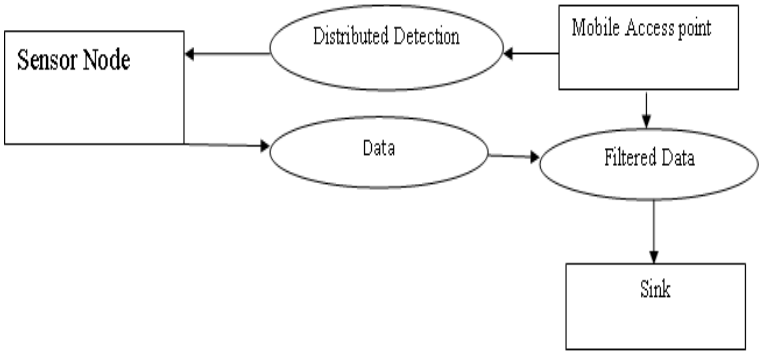

Fig 2: Component Module

Working scenario:

Sensor Node: Sensor nodes send sensed data to sink. If any attacker joins the network, he sends false data to sink to corrupt messages. We concentrate ona attack called Byzantine attack. Here when have two type of attackers ie.,Static attacker, who always sends false data to sink. He sends reverse information whenever data is requested. Dynamic attacker is a attacker who sends both valid information and invalid information to sink. Hence the system gets confused weather it is a valid sensor or invalid sensor.

Mobile Access Point: MAP is a mobile node which is used to collect data from sensor nodes. It uses Distributed Detection technique to sense weather a node is normal node or static attacker or dynamic attacker. Then it collects data from only valid nodes and sends aggregated data to sink.

Sink: Sink is a storage node. It gets data from mobile access point and stores it after separating aggregated messages.

Sequence diagram

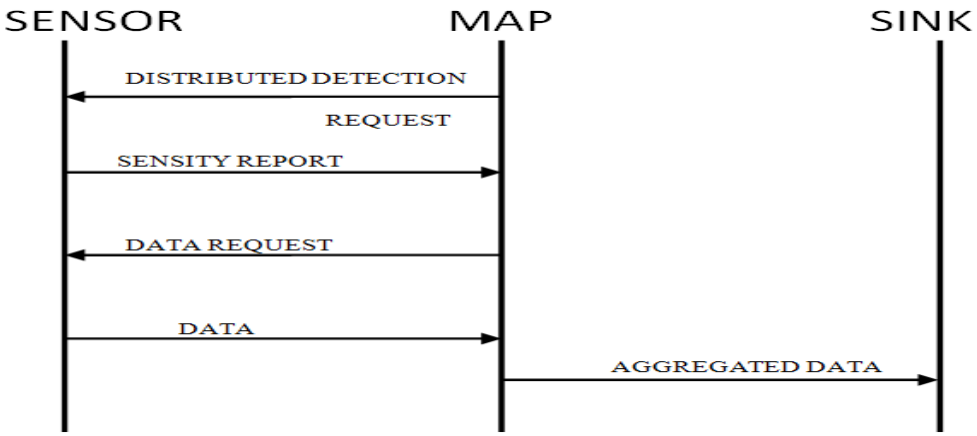

Fig 3: Sequences diagram for component module

IV. CONCLUSION

In this paper, we considered different types of byzantine attacks, we useddistributed detection method and based on prediction final result has been calculated. The information is collected only from valid nodes and then transfer to the destination. By this we can reduce loss of information this can be easy applied to large network and reduce byzantine failure. We believe that further research in detection systems will yield a variety of new detectors with different tradeoffs.

REFERENCES

[1] A. Bharathidasas and V. Anand, "Sensor networks: An overview," Technical report, Dept. of Computer Science, University of California at Davis, 2002.

[2] C. Chong and S. Kumar, "Sensor networks: evolution, opportunities, and challenges," Proceedings of the IEEE, vol. 91, no. 8, pp. 1247–2056, Aug. 2003.

[3] D. Martins and H. Guyennet, "Wireless sensor network attacks and security mechanisms: A short survey," 13th International Conference on Network-Based Information Systems, NBiS 2010, pp. 313–320, Sept. 2010.

[4] Y.-C. Wang and Y.-C. Tseng, "Distributed deployment schemes for mobile wireless sensor networks to ensure multilevel coverage," IEEE Transactions on Parallel and Distributed Systems, vol. 19, no. 9, pp. 1280 –1294, Sept. 2008.

[5]. M. Castro and B. Liskov. Practical Byzantine fault tolerance. In *Proceedings of OSDI'99*, pages 173-186, 1999.**]**

[6] A. Vempaty, K. Agrawal, H. Chen, and P. Varshney, "Adaptive learning of byzantines' behaviour in cooperative spectrum sensing," in *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, march 2011, pp. 1310 –1315.

[7] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of byzantine attacks," *Signal Processing, IEEETransactions on*, vol. 57, no. 1, pp. 16 –29, jan. 2009.

[8] H. Wang, L. Lightfoot, and T. Li, "On phy-layer security of cognitive radio: Collaborative sensing under malicious attacks," in *Information Sciences and Systems (CISS), 2010 44th Annual Conference on*, March 2010, pp. 1 –6.

[9] M. Abdelhakim, L. Zhang, J. Ren, and T. Li, "Cooperative sensing in cognitive networks under malicious attack," in*Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, May 2011, pp. 3004 –3007.

[10] Ming Yu, Mengchu Zhou, Wei Su, "A Secure Routing Protocol Against Byzantine Attacks forMANETs in Adversarial Environments", IEEE Vehicular Technology Society, 2008, IEEE