A Technique for Malicious Node Detection for Adaptive Data Fusion in Wireless Sensor Networks

Preethi M[*], Rashmi Purad[**], Kavya D S, Chandrakala H L****

[*]Department of Computer Science and Engineering, HKBK College of Engineering
[**]Department of Computer Science and Engineering, HKBK College of Engineering

DOI: 10.29322/IJSRP.8.6.2018.p7868
http://dx.doi.org/10.29322/IJSRP.8.6.2018.p7868

Abstract- Wireless sensor network requires secure and trusted communication. Due to lack of power supply and processing capability of sensor node ensuring security in wireless sensor network is a challenging task. The major attack in wireless sensor network is byzantine attack, where an opponent node has full control over some of the authenticated nodes and can perform arbitrary behavior to disturb the system. The key idea of this project is to ensure the delivery of accurate data in wireless sensor network with mobile access points (SENMA) for the reliable data fusion. In sensor network with mobile access points, the mobile node is used to collect data from sensor nodes. Mobile node uses distributed detection technique to sense weather a node is normal node or static attacker or dynamic attacker. Then it collects data from valid nodes only and sends aggregated data to sink.

Keywords- Byzantine Attack, SENMA, q-out-of-m scheme, WSN

I. INTRODUCTION

A Wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditional, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations .The development of wireless sensor network was originally motivated by military applications such as battlefield surveillance. However, Wireless sensor networks are now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health Monitoring, environment and habitat monitoring, healthcare application, 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 communication 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. A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm (several nodes may forward data).

II. LITERATURE SURVEY

Secure Hierarchical in-Network Aggregation in Sensor Network: ACM conf computer and comm security (ACM CCS 06) [1] ,The network aggregation is the process of performing queries on sensor network data. Most of time the aggregation algorithm assume that intermediate node are trusted ,but the standard threat model in sensor network security assume the attacker may control the fraction of node, which indirectly disturb the arbitrary behaviour of the system. This paper presents the secure hierarchical in-network data aggregation algorithm that guarantees to detect any manipulation of the aggregate at data compromised nodes. The algorithm incurs only o (Δlog2n) node congestion. The main algorithm is based on performing the sum aggregation securely; the algorithm also shows how to reduce secure MENDIAN count and AVERAGE to this primitive. It provides secure aggregation scheme for arbitrary aggregator topologies and multiple malicious nodes. The algorithm induces o (Δlog2n) node congestion where Δ is the maximum degree in the aggregation tree and provides the strongest security bound that can be proven for any secure aggregation scheme without making assumptions about the distribution of data values.

Reliable Data Fusion in Wireless Sensor Networks Under Byzantine Attacks Mai Abdelhakin Leonard E. Light Foot, Tongtong Li [2], It mainly concentrate about Byzantine attack in wireless sensor network with mobile access points. The part of active sensors is compromised to send false information, the effective method knows as q-out-of-m scheme is used to over-come this problem. This approach greatly reduces the computation complexity and keeps good performance, for the fixed percentage of malicious sensors, the

detection accuracy of the q-out-of-m detection, the system has the worst performance under the static attack where the malicious sensors always send false information .When the pre-detection is allowed, the system delivers much lower false alarm rates under both static and dynamic attacks.

Sensor Networks Evolution Opportunities and Challenges Chee-Yee Chong and Srikanta P. Kumar[3],Wireless micro sensor networks is one of the most important technologies for the 21st century. It mainly concentrates on history of research in sensor networks, technology trends, new applications, research issues in wireless sensor networks. It presents two important programs of the Defence Advanced Research Project Agency (DARPA) that is Distributed Sensor Networks (DSN) and the sensor Information Technology (sens IT) Programs. Sensor networks are widely used in new applications such as infrastructure security, habitat monitoring, and traffic control. Technical challenges in sensor network development include network discovery control and routing, collaborative signal and information processing, tasking and querying and security. It also presents some recent research results in sensors network algorithm that includes localized algorithms and directed diffusion, distributed tracking in ad hoc networks and distributed classification using local agents.

SPINS: Security Protocols for Sensor Networks Edge Adrian Perrig, Robert Szewzyk , J.D.Tygar, Victor Wen and David E Culler [4],As we all know wireless sensor networks edge closer towards wide-spread deployment, security issues becomes a central concern, so far, much research has focused on making sensor networks feasible and useful, as has not concentrated on security. It mainly concentrates on security building blocks optimized for research constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and TESLA.SNEP provides the following important baseline security primitives: Data confidentiality, two-party data authentication and data freshness. TESLA is a new protocol which provides authenticated broadcast for severely resource constrained environments. The above two protocols are implemented and show that they are practical even on minimal hardware. The performance of the protocol suite easily matches the data rate of the network.

III. EXISTING SYSTEM

Here The centralized sensor network architecture known as sensor network with mobile access points (SENMA) is considered where the network is composed of n-power limited sensor nodes and a powerful mobile access point. The nodes are randomly and uniformly distributed over the network, and the mobile access point traverses the network to communicate with all sensing nodes. The sensor network with mobile access point performs distributed detection. Each senor node detects the presence of the target object by applying an application dependent detection algorithm knows as energy detection and sends one-bit hard decision report to the mobile access point, which makes the final decision accordingly.

This hard decision technique reduces the transmission and processing burden of the sensor network. But the disadvantage existing system is since the centralized architecture is used in sensor network, if the central node fails then the entire network will collapse. There no scalability and efficiency in wireless sensor network. It is not suitable for large size networks.

IV. PROPOSED SYSTEM

The simplified linear q-out-of-m scheme is proposed that can easily applied to large size networks. The proposed linear approach can achieve satisfying accuracy with low false alarm rate. The closed-form solution knows as q-out-of-m fusion scheme based on the central limit theorem is proposed for easier and more flexible distributed data fusion that can easily adapt to unpredictable environment and cognitive behavior of malicious nodes, the linear approach and closed-form solution shows that under a fixed alarm rate of both approaches diminishes exponentially as the network size increases. The proposed malicious detection approaches can easily identify malicious sensors accurately if sufficient observation time is allowed. The adaptive data fusion scheme can improve the system performance significantly under both static and dynamic attack strategies.

V. SYSTEM IMPLEMENTATION

List of modules
It mainly consist of three modules

1. Sensor node
2. Mobile Access Point(MAP)
3. Sink

Sensor nodes send sensed data to sink. If any attacker joins the network, he sends false data to sink to corrupt messages. We concentrate on attack called Byzantine attack. Here we have two type of attackers i.e., Static attacker, who always sends false data to sink. He sends reverse information whenever data is requested. Dynamic attacker is an 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.
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 is a storage node. It gets data from mobile access point and stores it after separating aggregated messages.

Performance Evaluation

In these modules, flexibility and scalability the proposed work is evaluated. Proposed work show shows better performance under both static and dynamic byzantine when compared to existing system.

VI. RESULTS

Connection establishment between mobile access point and sink

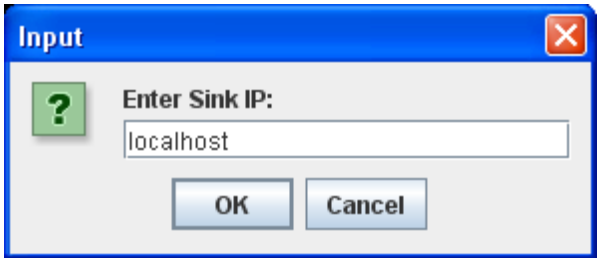

Fig.1: Aggregated message is forwarded to sink

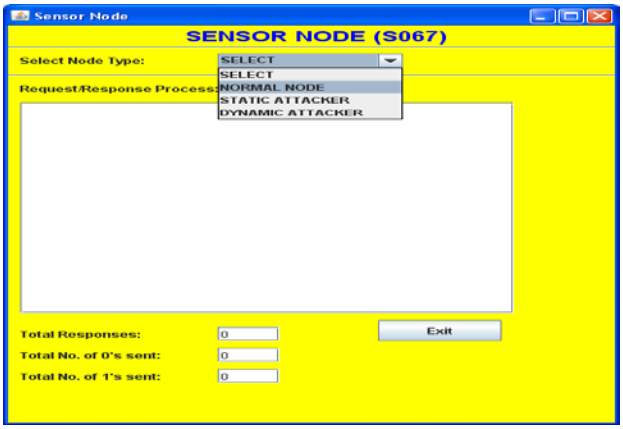

Fig.2: Sensor node creation

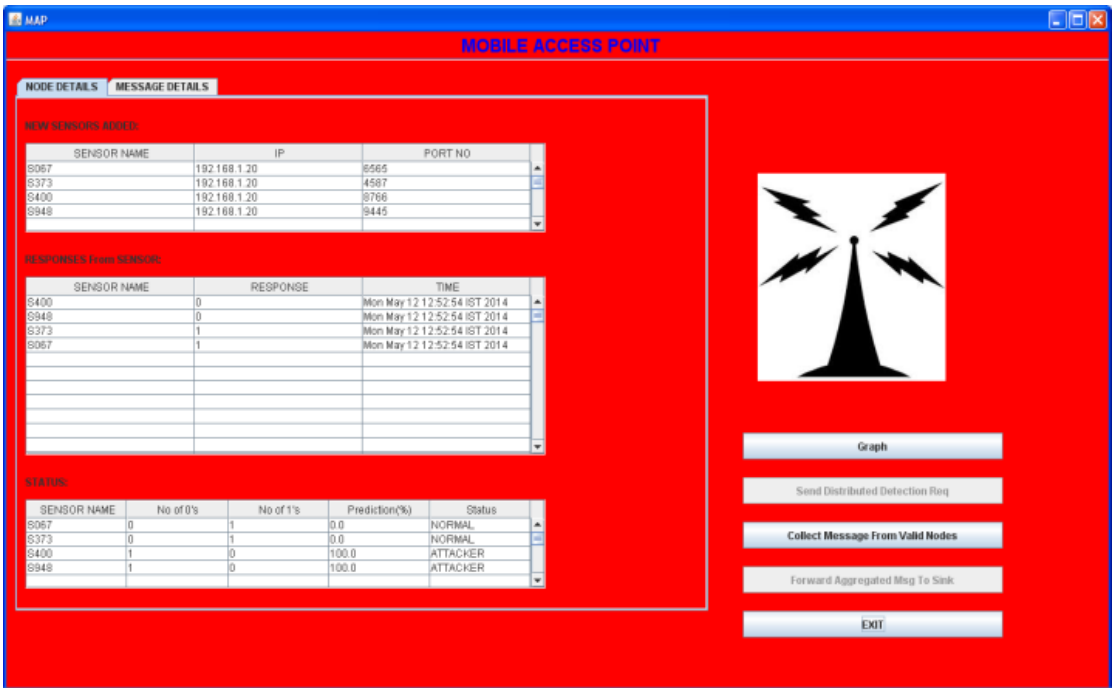

Fig.3: Mobile access point shows prediction values normal nodes and byzantine attackers

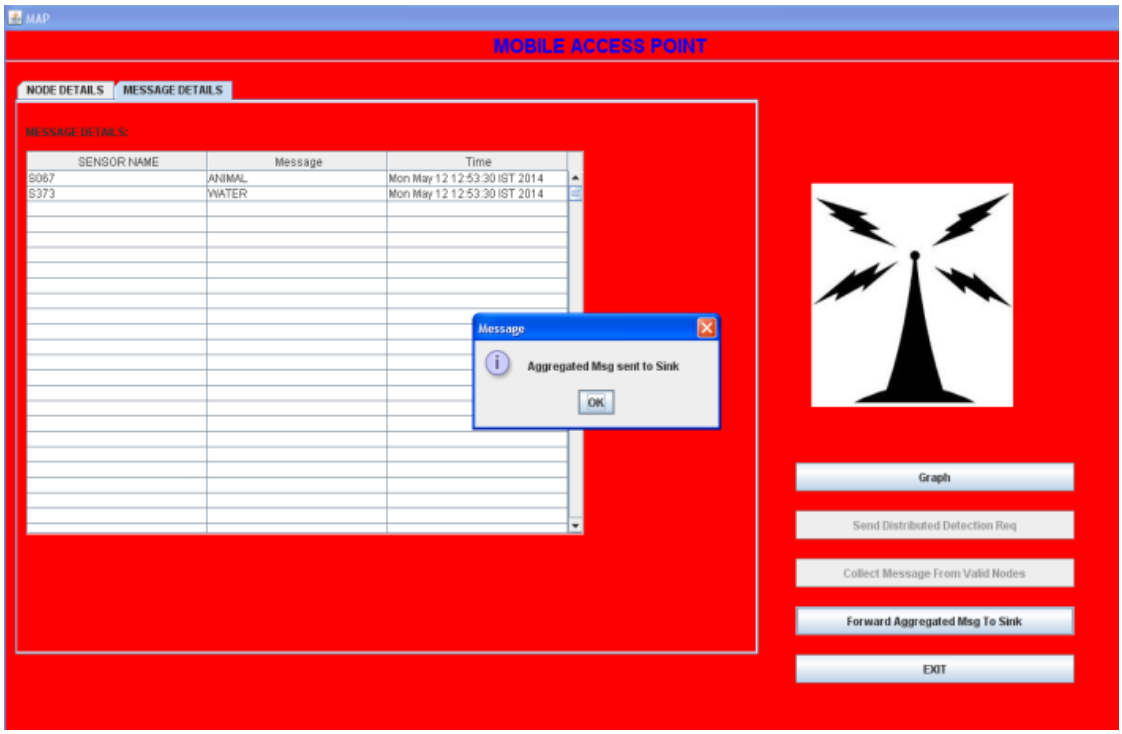

Fig.4: Aggregated Messages sent to MAP

VII. CONCLUSION

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

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

REFERENCES

[1] Mai Abdelhakim , Leonard E. Lightfoot, Jian Ren , Senior Member , "Distributed Detection in Mobile Access Wireless Sensor Networks under Byzantine Attacks "IEEE Transactions on Parallel and Distributed systems, vol. 25, no. 4, April 2014
[2] 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.
[3] C. Chong and S. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," Proc. IEEE, vol. 91, no. 8, pp. 1247-2056, Aug. 2003.
[4] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler, "Spins: Security Protocols for Sensor Networks," Wireless Networks, Vol. 8, pp. 521-534, A:1016598314198, Sept. 2002.
[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]H. Kumar, D. Sarma, and A. Kar, "Security Threats in Wireless Sensor Networks," IEEE Aerospace and Electronic Systems Magazine, Vol. 23, no. 6, pp. 39-45, June 2008.

AUTHORS

First Author – Preethi M, M.Tech(CSE), HKBK College of Engineering and preethim.cs@hkbk.edu.in
Second Author – Rashmi Purad, M.Tech(CSE), HKBK College of Engineering and rashmip.cs@hkbk.edu.in
Third Author – Kavya D S, M.Tech(CSE), HKBK College of Engineering and kavyads.cs@hkbk.edu.in
Fourth Author – Chandrakala H L, M.Tech(CNE), HKBK College of Engineering and chandrakalahl@gmail.com

.

Correspondence Author – Preethi M, preethim.cs@hkbk.edu.in, preethi.m.68@gmail.com , 8904966180