ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

"Privacy Preserving Data Aggregation that avoids malicious modification of sensor data"

Prajna Mayadi[1], Chinmai Shetty[2]

M-Tech Scholar, Department of CSE, Alvas Institute of Engineering and Technology, Moodbidri, India[1]

Assistant Professor, Department of CSE, Alvas Institute of Engineering and Technology, Moodbidri, India[2]

Abstract: Wireless sensor network consists of a huge number of tiny electromechanical sensor devices that are capable of sensing, computing and communicating. These electromechanical sensor devices can be made use for gathering sensory information, like measurement of temperature from an extensive geographical area. Many features of the wireless sensor networks have given rise to challenging problems. Sensor nodes are deployed in open hostile environment in WSN applications. An adversary can easily compromise sensor nodes due to their unattended nature. Adversaries can inject false data reports into the WSN through compromised nodes. The false data reports lead the en-route nodes and the base station to make false decision. False decision depletes the energy of en-route nodes and the base station.

Keywords: WSN, sensor nodes, aggregator.

I. INTRODUCTION

Wireless sensor network (WSN) is composed by a large number of spatially distributed autonomous sensors to monitor environmental conditions such as temperate, pressure, pollutant [1], with the features of multi-hop, self-organized and resource-constrained. Usually, It's distributed in a large -scale field to gather data in a severe environment, and its topologies change dynamically and unpredictably. WSNs are susceptible to a large number of security threats, because of the communication, computation and delay constraints of most applications [2].

In-network aggregation is a well known technique to achieve energy efficiency when propagating data from information sources (sensor nodes) to multiple sinks. The main idea behind in-network aggregation is that, rather than sending individual data items from sensors to sinks, multiple data items are aggregated as they are forwarded by the sensor network. Data aggregation is application dependent, i.e., depending on the target application, the appropriate data aggregation operator (or aggregator) will be employed. From the information sink's point of view, the benefits of in-network aggregation are that in general it yields more manageable data streams avoiding overwhelming sources with massive amounts of information, and performs some filtering and pre-processing on the data, making the task of further processing the data less time and resource consuming[3]. An important issue in applying data aggregation is to avoid tampering of the nodes so that the base station can get the correct data aggregation result. To accomplish malicious aggregator identification, nodes performs aggregation recalculation.

Data privacy can be simply defined as a process in which private data can be overheard and decrypted by adversaries or other trusted participating sensor nodes, but it can still provide a mechanism that prevents them from recovering sensitive information, i.e., control disclosure of any information about the data. To achieve data privacy, it is required to protect transmission of a node's private data from its neighbouring nodes.

II. PROBLEM STATEMENT

The proposed system presents method to detect for false data detection with data aggregation and confidentiality when two consecutive nodes are compromised. To support data aggregation along with false data detection, the monitoring nodes of every data aggregator also conduct data aggregation and compute the corresponding small-size message authentication codes for data verification at their pair mates.

III. DATA AGGREGATION IN WSN

Data aggregation protocols aim to combine and summarize data packets of several sensor nodes so that amount of data transmission is reduced.An example data aggregation scheme is presented in Fig. 1 where a group of sensor nodes collect information from a target region. When the base station queries the network, instead of data to base station, one of the sensor nodes, called data aggregator, collects the information from its neighbouring nodes, aggregates them (e.g., computes the average), and sends the aggregated data to the base station over a multihop path.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

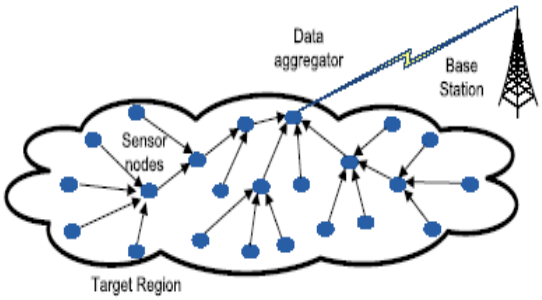
Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

3.1 Approaches to data aggregation

Tree-Based Approach [1]: In the tree-based approach perform aggregation by constructing an aggregation tree, which could be a minimum spanning tree, rooted at sink and source nodes are considered as leaves. Each node has a parent node to forward its data. Flow of data starts from leaves nodes up to the sink and therein the aggregation done by parent nodes.

Cluster-Based Approach [2]: In cluster-based approach, whole network is divided in to several clusters. Each cluster has a cluster-head which is selected among cluster members. Clusterheads do the role of aggregator which aggregate data received from cluster members locally and then transmit the result to sink.



3.2Wireless Sensor Networking Requirements and Challenges

For a wireless sensor network to deliver real-world benefits, it must support the following requirements in deployment: scalability, reliability, responsiveness, mobility, and power efficiency. The complex inter-relationships between these characteristics is a balance; if they are not managed well, the network can suffer from overhead that negates its applicability in the real world. In order to ensure that the network supports the application's requirements, It is important to understand how each of the wireless sensor networking characteristics affects reliability.

Table 1: Essential Requirements of Wireless Sensor Networks

Requirements	Description
Reliability	The ability of the network to ensure reliable data transmission in a state of continuous change of network structure.
Scalability	The ability of the network to grow, in terms of the number of nodes, without excessive overhead.
Responsiveness	The ability of the network to quickly adapt itself to changes in topology.
Mobility	The ability of the network to handle mobile nodes and changeable data paths.
Power efficiency	The ability of the network to operate at extremely low power levels.

IV. ROUTING

Multihop routing is a critical service required for WSN. Because of this, there has been a large amount of work on this topic. Internet and MANET routing techniques do not perform well in WSN. Internet routing assumes highly reliable wired connections so packet errors are rare; this is not true in WSN. Many MANET routing solutions depend on symmetric links (i.e., if node A can reliably reach node B, then B can reach A) Between neighbours; this is too often not true for WSN. These differences have necessitated the invention and deployment of new solutions. For WSN, which are often deployed in an ad hoc fashion, routing typically begins with neighbour discovery. Nodes send rounds of messages (packets) and build local neighbour tables. These tables include the minimum information of each neighbour's ID and location. This means that nodes must know their geographic location prior to neighbour discovery. Other typical information in these tables includes nodes' remaining energy, delay via that node, and an estimate of link quality. Once the tables exist, in most WSN routing algorithms messages are directed from a source location to a destination address based on geographic coordinates, not IDs. A typical routing algorithm that works like this is Geographic Forwarding (GF) .In GF, a node is aware of its location, and a message that it is "routing" contains the destination address. This node can then computes which neighbour node makes the most progress towards the destination by using the distance formula from geometry. It then forwards the message to this next hop. In variants of GF, a node could also take into account delays, reliability of the link and remaining energy.

.

REFERENCES

[1]. Larry C. Llewellyn, Kenneth M. Hopkinson, and Scott R.Graham, "Distributed Fault-Tolerant Quality of Wireless Networks", IEEE Transactions on Mobile Computing, Vol.10, pp.175-190, 2010.

[2]. Boukerche, L. Xu and K. EI-Khatib, "Trust-based security for wireless ad hoc and sensor networks", Computer Communications, vol. 30, pp.2413-2427, 2007.

[3]. Mohamed Watfa, William Daher and Hisham Al Azar,"A Sensor Network Data Aggregation Technique" International Journal of Computer Theory and Engineering, Vol. 1, No. 1, April 2009 1793-821X

[4]. Hongjuan Li, Keqiu Li, Wenyu Qu, Ivan Stojmenovic, Secure and energy efficient data aggregation with malicious aggregator identification in wireless sensor networks, in: Proceedings of the 11th International Conference on Algorithms and Architectures for Parallel Processing—Volume Part I, 2011,pp. 2–13

[5]. 40. S. Madden, M.J. Franklin, J.M. Hellerstein, W. Hong, TAG: A tiny aggregation service for ad-hoc sensor networks.ACM SIGOPS Oper. Syst., Rev. **36**(SI), 131–146 (2002).

[6]. R. Rajagopalan, P. Varshney, Data-aggregation techniques in sensor networks: A survey. IEEE Commun. Surv. Tutor. **8**(4), 48–63 (2006).

[7]. Priyanka S. Fulare and Nikita Chavhan (2011) ,"False Data Detection in Wireless Sensor Network with Secure Communication".In:. InternationalJournal of Smart Sensors and Ad Hoc Networks (IJSSAN), Vol.1.

[8]. S. Chaitanya Rami Reddy, P. Ravinder Kumar ,"Implementation of DataAggregation and Authentication in Wireless Sensor Networks", InternationalJournal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-5, November 2012.