False Data Detection using Trusted Group Membership Service

B.Gnanavel, N.Kumaratharan

Department of Information Technology
Sri Venkateswara College of Engineering
Sriperumbudur 602105, India

Abstract - Wireless sensor networks are vulnerable to many types of security attacks, including false data injection, data forgery, and eavesdropping. Sensor nodes can be compromised by intruders, and the compromised nodes can distort data integrity by injecting false data. The transmission of false data depletes the constrained battery power and degrades the bandwidth utilization. False data can be injected by compromised sensor nodes in various ways, including data aggregation and relaying. Because data aggregation is essential to reduce data redundancy and to improve data accuracy, false data detection is critical to the provision of data integrity and efficient utilization of battery power and bandwidth. In addition to false data detection, data confidentiality is required by many sensor network applications to provide safeguard against eavesdropping. The proposed work is to integrate the detection of false data with data aggregation and confidentiality. Data confidentiality prefers data to be encrypted at the source node and decrypted at the destination. However, data aggregation techniques usually require any encrypted sensor data to be decrypted at data aggregators for aggregation.

Keywords - data confidentiality, data aggregation, false data detection

I. INTRODUCTION

Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements. These networks will consist of hundreds or thousands of self-organizing, low-power, low-cost wireless nodes deployed to monitor and affect the environment. Potential applications include burglar alarms, inventory control, medical monitoring and emergency response, monitoring remote or inhospitable habitats, target tracking in battlefields, disaster relief networks, early fire detection in forests, and environmental monitoring. Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. This leads to a very demanding environment to provide security. Public-key cryptography is too expensive to be usable, and even fast symmetric-key ciphers must be used.

Each bit transmitted consumes much power, and as a consequence, any message expansion caused by security mechanisms comes at significant cost. Wireless sensor network (WSN) is an area of great interest to both academia and industry. They open the door to a large number of military, industrial, scientific, civilian and commercial applications. They allow cost-effective sensing especially in applications where human observation or traditional sensors would be undesirable, inefficient, expensive, or dangerous. Wireless sensors have limited energy and computational capabilities, making many traditional security methodologies difficult or impossible to utilize. Also, they are often deployed in open areas, allowing physical attacks such as jamming or node capture and tampering. There are lot of researches is done in security issues. Some of the terms addressing this issue are discussed. Data confidentiality prefers data to be encrypted at the source node and decrypted at the destination. However, data aggregation techniques usually require any encrypted sensor data to be decrypted at data aggregators for aggregation. The proposed work depicted in Fig. 1 is to integrate the detection of false data with data aggregation and confidentiality. Data confidentiality prefers data to be encrypted at the source node and decrypted at the destination. However, data aggregation techniques usually require any encrypted sensor data to be decrypted at data aggregators for aggregation.

Data detection techniques consider false data injections during data forwarding only and do not allow any change on the data by data aggregation. Data detection algorithms address neither data aggregation nor confidentiality. Although they could be modified easily to support data confidentiality, it is a challenge for them to support the data aggregation that alters data. Random key distribution protocols such as allow key establishment using multi hop communication. Some other techniques that allow non neighboring sensor nodes to establish pair wise keys of the following reason, random key distribution protocols. Each data aggregator and its neighboring...
nodes are assumed to establish a group key using an group key establishment scheme. The propose work is discussed further. Data confidentiality increase the communication overhead, simulation results show that DAA can still reduce the amount of transmitted data aggregation and early detection. Data aggregation is implemented in wireless sensor networks to eliminate data redundancy, reduce data transmission, and improve data accuracy. A joint data aggregation and false data detection technique has to ensure that data are altered by data aggregation. Data confidentiality prefers data to be encrypted at the source node and decrypted at the destination. Data aggregation techniques usually require any encrypted sensor data to be decrypted at data aggregators for aggregation. Data confidentiality during data forwarding between every two consecutive data aggregators, the aggregated data are encrypted at data aggregators. DAA’s communication overhead is less compared to the false data detection scheme.

II. RELATED WORK

The existing false data detection algorithm \cite{1, 2} addresses neither data aggregation nor confidentiality. Although they could be modified easily to support the data confidentiality, whereas data aggregation is a much more challenging task that alters data. The basic idea behind the false data detection algorithm is to form pairs of sensor nodes such that one pair mate computes a message authentication code (MAC) of forwarded data and the other pair mate later verifies the data using the MAC of forwarded data. In this scheme, any data change between two pair mates is considered as false data injection, and therefore, data aggregation is not allowed if it requires alterations in the data. Hence the false data detection algorithm cannot be implemented when a data aggregator between two pair mates changes the data. Data aggregation is implemented in wireless sensor networks to eliminate data redundancy, reduce data transmission, and improve data accuracy. Data aggregation results in better bandwidth and battery utilization \cite{3}, which enhances the network lifetime because communication constitutes 70 percent of the total energy consumption of the network \cite{4}. Although data aggregation is very useful, it could cause some security problems because a compromised data aggregator may inject false data during data aggregation. When data aggregation is allowed, the false data detection technique should determine correctly whether any data alteration is due to data aggregation or false data injection. To detect false data injections, data authentication schemes that employ multiple MACs are presented in \cite{2, 5}. The statistical en-route detection scheme \cite{2}, called SEF, enables relaying nodes and base station to detect false data with a certain probability. In the interleaved hop-by-hop authentication scheme \cite{3}, any packet containing false data injected by T compromised sensor nodes is detected by those T+1 sensor nodes that collaborate to verify data integrity. In the interleaved hop-by-hop authentication scheme, sensor nodes are not allowed to perform data aggregation during data forwarding. The Commutative Cipher based En-route Filtering scheme (CCEF) \cite{4} drops false data en-route without symmetric key sharing. With the use of a commutative cipher, a forwarding node can use the witness key to verify the authenticity of the reports without knowing the original session key. In the dynamic en-route filtering scheme \cite{5}, false data are filtered in a probabilistic nature in the sense that a forwarding node can validate the authenticity of a report only if it has a corresponding authentication key. A legitimate report is endorsed by multiple sensor nodes using their distinct authentication keys from one-way hash chains. Secure data aggregation problem is studied extensively. In the security mechanism detects node misbehaviors such as dropping or forging messages and transmitting false data. In random sampling mechanisms and interactive proofs are used to check the correctness of the aggregated data at base station. In sensor nodes first send data aggregators the characteristics of their data to determine which sensor nodes have distinct data, and then those sensor nodes having distinct data send their encrypted data. Several key establishment protocols are developed for sensor networks which offer direct key establishment for neighboring nodes and path key establishment for sensor nodes that are multiple hops away from each other. The proposed work is to integrate the detection of false data with data aggregation and confidentiality. Data confidentiality prefers data to be encrypted at the source node and decrypted at the destination. Data aggregation is implemented in wireless sensor networks to eliminate data redundancy, reduce data transmission, and improve data accuracy. A joint data aggregation and false data detection technique has to ensure that data are altered by data aggregation. However, data aggregation techniques usually require any encrypted sensor data to be decrypted at data aggregators for aggregation.
III. FALSE DATA DETECTION

![Diagram of False Data Detection](image)

**A. Networking**

Client-server computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await (listen to) incoming requests.

**B. Data Integrity**

The compromised nodes can distort data integrity by injecting false data. The transmission of false data depletes the constrained battery power and degrades the bandwidth utilization. To verify data integrity, in the interleaved hop-by-hop authentication scheme, sensor nodes are not allowed to perform data aggregation during data forwarding.

**C. Sensor Networks**

Previously known techniques on false data detection do not support data confidentiality and aggregation, even though they are usually essential to wireless sensor networks. However, this paper has presented the novel security protocol DAA to integrate data aggregation, confidentiality, and false data detection. The importance of data aggregation in a densely deployed sensor network, it is assumed that MDAA is a modified version of DAA such that it is the same as DAA, except that MDAA does not perform any data aggregation at all. That is, DAA mitigates the redundant data at data aggregators by implementing data aggregation. It is to enable every sensor node to be capable of both aggregating and forwarding data in order to improve network security and efficiency.

**D. Data aggregation**

Data aggregation is essential to reduce data redundancy and/or to improve data accuracy, false data detection is critical to the provision of data integrity and efficient utilization of battery power and bandwidth. Data aggregation techniques usually require any encrypted sensor data to be decrypted at data aggregators for aggregation. The existing false data detection algorithms address neither data aggregation nor confidentiality. Although they could be modified easily to support data confidentiality, it is a challenge for them to support the data aggregation that alters data. Data aggregation is implemented in wireless sensor networks to eliminate data redundancy, reduce data transmission, and improve data accuracy. Data aggregation results in better bandwidth and battery utilization which enhances the network lifetime. Data aggregation is very useful; it could cause some security problems because a compromised data aggregator may inject false data during data aggregation. When data aggregation is allowed, the false data detection technique should determine correctly whether any data alteration is due to data aggregation or false data injection.

**E. Data detection**

The false data detection algorithm in is to form pairs of sensor nodes such that one pair mate computes a message authentication code (MAC) of forwarded data and the other pair mate later verifies the data using the MAC. Data aggregation is allowed, the false data detection technique should determine correctly whether any data alteration is due to data aggregation or false data injection. A joint data aggregation and false data detection technique has to ensure that data are altered by data aggregation only. A data aggregation and authentication protocol (DAA) to provide false data detection and secure data aggregation against up to compromised sensor nodes. DAA provides secure data aggregation, data confidentiality, and false data detection by performing data aggregation at data aggregators and their neighboring nodes and verifying the aggregated data during data forwarding between two consecutive data aggregators. The security of Algorithm SDFC is analyzed with respect to its false data detection ability. In Algorithm SDFC, compromised nodes can inject false data during data aggregation or data...
forwarding. When a sensor node is compromised, the intruder is assumed to access all the available security information such as cryptographic keys of the node.

IV. CONCLUSION AND FUTURE WORK

In wireless sensor networks, compromised sensor nodes can distort the integrity of data by injecting false data. Previously known techniques on false data detection do not support data confidentiality and aggregation, even though they are usually essential to wireless sensor networks. However, this paper has presented the novel security protocol DAA to integrate data aggregation, confidentiality, and false data detection. DAA appends two FMACs to each data packet. To reduce the communication overhead of algorithm SDFC, the size of each FMAC is kept fixed. Each FMAC consists of sub MACs to safeguard the data against up to compromised sensor nodes. The performance analysis indicates that the computational and communication overhead of DAA is not substantial, thereby making the implementation of DAA feasible. The simulation results show that the amount of transmitted data is reduced by up to 60%, leading to a significant improvement in bandwidth utilization and energy consumption. As for the future research, it is to enable every sensor node to be capable of both aggregating and forwarding data in order to improve network security and efficiency.

REFERENCES


