Journal Of Harmonized Research (JOHR)

Journal Of Harmonized Research in Engineering
1(1), 2013, 29-33

ISSN 2347 – 7393

Original Research Article

SECURE AND EFFICIENT DATA AGGREGATION ARCHITECTURE

Aparna Chandran*

Department of Computer Science and Engineering
Nehru College of Engineering and Research Centre
Pampady, Thiruvilwamala, Thrissur, Kerala

ABSTRACT: A wireless sensor network consists of spatially distributed autonomous and efficient sensors to monitor environmental conditions and physical conditions. In wireless sensor network, one of the widely used techniques is data aggregation. There has been many related papers and works proposed to address this data aggregation technique. However less of them pay attention to the property of data integrity. An attacker can simply modify data to affect the decision of base station by compromised nodes. Therefore, a new efficient and secure data aggregation architecture is proposed to find the compromised nodes and help the base station to verify the final results.

Keywords- Data Aggregation, Data Integrity, Sensor

Introduction

The wireless sensor network contains one or several base stations and hundreds of sensor nodes. Wireless sensor network applications include manufacturing machinery performance monitoring, ocean and wildlife monitoring, fire monitoring, building safety and earthquake monitoring and many military applications. A major benefit of these systems is the performance in network processing to reduce large streams of raw data into useful collected information. The sensor nodes in these networks have severe constraints such as limited processing power, limited bandwidth, short battery life and physically prone to external threats. Since the communication cost is much more than the computation cost in wireless sensor networks, many kinds of data aggregation schemes are proposed. Data aggregation is the process of aggregating the sensor data using aggregation approaches. The main goal of data aggregation protocols is to collect and aggregate data in an energy efficient manner so that network lifetime is enhanced. The internal nodes in wireless sensor networks can forge, modify and drop messages easily in accordance with the topology by an attacker. These actions could induce a bias to the final result in the wireless

For Correspondence:
aparnachandran1188@gmail.com
Received on: August 2013
Accepted after revision: September 2013
Downloaded from: www.johronline.com

sensor network. In addition, an attacker could also learn the contents of the packets by overhearing messages. The previous data aggregation protocols do not provides any security against these attacks. Therefore, a new efficient and secure data aggregation architecture is proposed to resist these attacks and the base station can verify the final results without any bias.

Sensor Network Architecture

Westhoff *et al.*(2006) states that one needs to logically separate sensor nodes, forwarding nodes, aggregator nodes, and the sink node, which initiates the monitoring and data collecting process. Aggregator nodes and forwarding nodes belong to the backbone, whereas sensor nodes persist in sleep mode until the sink node initiates a process which requires a subset of nodes to contribute. The sink node may either be the connection to the fixed network or the end point for the data collection process. A typical sensor network has hundreds to several thousands of sensor nodes. Each sensor node is typically low-cost, limited in computation and information storage capacity, highly power constrained and communicates over a short range wireless network interface. Individual sensor nodes communicate locally with neighboring sensors, and send sensor readings over the peer-to-peer sensor network to the base station. The three communication patterns are node to node communication, node to base station communication, base station to node communication. In this paper, all the sensor nodes are classified into base stations, leaf nodes and aggregators. The leaf nodes are the nodes which focus on sensing and reporting data. Aggregators are the internal nodes that focus on aggregating and relaying data. The base station analyzes the receiving data and detects the existence of emergent events and attacks.

Source Location Privacy

Kamat *et al.* (2005) defined privacy as the guarantee that information, in its general sense, is observable or decipherable by only the person intentionally meant to observe or decipher it. The phrase “in its general sense” is meant to imply that there may be types of information besides the message content that are associated with a message transmission. The privacy threats that exist for sensor networks are categorized into two broad classes. The two classes are content oriented security or privacy threats and contextual privacy threats. Content oriented security or privacy threats are issues that arise due to the ability of the adversary to observe and manipulate the exact content of packets being sent over the sensor network whether these packets correspond to actual sensed data or sensitive lower layer control information. Contextual privacy issues associated with sensor communication have not been as thoroughly addressed as content oriented security. In contrast to content oriented security, the issue of contextual privacy is concerned with protecting the context associated with the measurement and transmission of sensed data.

There are three types of privacy issues in network communication. The three privacy issues are content privacy, identity privacy and location privacy. Content privacy threat is any means by which an adversary can determine the meaning of a communication exchange. It might not be necessary for the adversary to be able to read the message. Identity privacy threat is a method that allows an adversary to deduce the identities of entities involved in a communication exchange. Location privacy is a method that allows an adversary to determine the location of a communicating entity [3].

Data Aggregation Architecture

After the secure deployment of sensor nodes, the base station requests all sensor nodes to construct a topology tree. For the construction of the topology, the base station broadcasts a topology construction message to all sensor nodes. The detailed format of the message contains source address, original address, sequence number, hop count, sensing type and

aggregation function. Before broadcasting this message, the base station sets the source address and original address as itself. The hop count is represented as the number of hops to the base station. The base station initializes hop count as zero. Upon receiving the message, each sensor node checks whether it receives the request or not. If the message is not a request, it marks the source node of this message as its parent. The sensor node also records the hop count into its storage and then increases the variable hop count by one. If a node receives the same request again, it compares the new hop count with its original hop count. If the new hop count is larger than the original hop count, it records the source node of this message as its child. If the new hop count and original hop count are equal, then it records the source node as its sibling. If the new hop count is smaller than the original hop count, it records the source node as its ancestor. After the topology construction, each node can be aware of its parent, sibling and children in the topology. Each node also informs the base station the relations with its neighbors along with its hop count. Hence, the base station can know the topology of the whole networks.

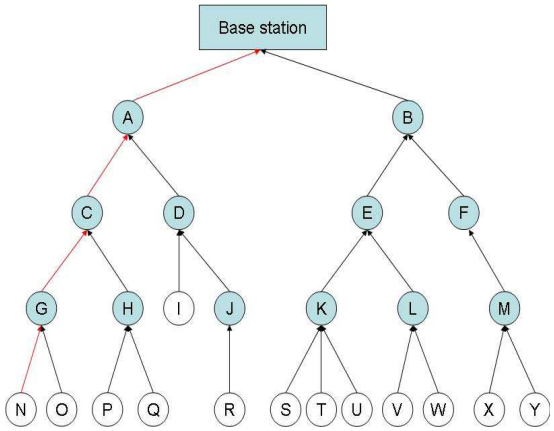

Figure 1: Data processing with single-path routing

Key Predistribution Schemes

Chan *et al.* (2003) proposed three new mechanisms in the framework of random key predistribution to address the bootstrapping problem. The first mechanism is the q-composite random key predistribution scheme, which achieves great security under small scale attack while trading off increased vulnerability in the face of a large scale physical attack on network nodes. The second mechanism is the multi-path key reinforcement scheme, which substantially increases the security of key setup such that an attacker has to compromise many more nodes to achieve a high probability of compromising any given communication. The third mechanism is the random-pairwise keys scheme, which assures that, even when some number of nodes has been compromised, the remainder of the network remains fully secure. This random-pairwise key scheme enables node-to-node mutual authentication between neighbors and quorum-based node revocation.

Efficient bootstrapping of secure keys is of critical importance for secure sensor network applications. Local processing of sensor data requires secure node to node communication. Each of these three schemes represents a different tradeoff in the design space of random key protocols. The choice of which scheme is best for a given application will depend on which trade-off is the most appealing. The q-composite scheme achieves significantly improved security under small scale attack at the cost of greater vulnerability to large scale attack. The multipath reinforcement scheme improves security at the cost of network communication. The random pairwise scheme has the best security properties of the three schemes. It possesses perfect resilience against node capture attacks as well as support for node based revocation and resistance to node replication.

DATA PROCESSING

After the topology construction and key generation, each sensor node knows all its neighbors. In the next step, leaf nodes and aggregators perform different data processing

according to the contents of messages. The contents of messages can be classified as an emergent event or a usual event. When an emergency happens, sensor nodes could transmit the emergent event by single routing path or multiple routing paths. If the message is a usual event, then it is only sent by one path. After sensing the data, the leaf nodes transmit the readings to aggregators. An aggregator receives messages from its children and decrypts those messages. Initially, aggregator checks whether there is any abnormal value exists in the message. If there is any abnormal value exists, then aggregator encrypts the original sender's identifier, sensing value and the timestamp and forms an encrypted unit along with the original message authentication code. If the aggregator is not receiving an emergent event, it just aggregates these sensing data, encrypts the data with its pairwise key and forwards to its parent. These steps continue until the base station receives all aggregated results.

Whenever the base station receives messages from aggregators, it can verify the correctness and validity. If the base station receives the emergent message from aggregator, it can identify the original sender at first and verify the message authentication code value. If the message authentication code is correct and valid, the base station accepts the result and replies an acknowledgement to the sender immediately. If the message authentication code is not valid or correct, the base station can be aware that the sensor network suffers some attacks and it drops the receiving message. The base station does not send any acknowledgment as reply to the sender and it records the suspicious nodes into table. In order to distinguish a normal node from a compromised node, base station maintains a table to record the behaviors of each node.

FEATURES OF THE ARCHITECTURE

The main security properties of this architecture are data confidentiality, data integrity, replay attack resistance, dropping resistance and forging detection. Data confidentiality means an adversary tries to overhear transmitted packets and learn information from those packets. Data integrity means an adversary would try to alter a receiving message and send that message in order to skew the aggregated value in wireless sensor networks. Forging means an adversary could impersonate a leaf node and forge an emergent message. Whenever an aggregator receives the falsified message from the leaf node, it cannot verify the correctness of the data.

Conclusion

The paper notifies about a less resource secure data aggregation architecture for wireless sensor networks. A wireless sensor network contains one or several base stations and hundreds of sensor nodes. Many data aggregation schemas are proposed to reduce the communication cost in wireless sensor networks. The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. In wireless sensor network, an attacker can easily forge, modify and drop the messages by the compromised nodes. The previous data aggregation protocols do not provides any security against these attacks. Therefore, a lightweight secure architecture is proposed to resist these attacks and provides an end to end aggregate authentication. In this proposed protocol, all the data are encrypted and an attacker cannot learn that data of children even if an aggregator is compromised. This scheme proposes a new encryption scheme that allows intermediate sensors to aggregate encrypted data of its children without having to decrypt and provides stronger privacy than a simple aggregation scheme using hop-by-hop encryption.

ACKNOWLEDGMENT

This work is supported by my research guide. I am very thankful to my research guide Mr. Arundas K.V., Lead Android Programmer, BlackJack Apps, Trivandrum, for his support and guidance.

References

[1] Chan, H., A. Perrig and D. Song, (2003). "Random Key Predistribution Schemes for Sensor Networks" Proceedings of the 2003 IEEE Symposium on Security and Privacy (SP'03), Berkeley, US, pp.197-213.

[2] Kamat, P., Y. Zhang, W. Trappe and C. Ozturk, (2005). "Enhancing Source- Location Privacy in Sensor Network Routing" Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), Columbus, US, pp.599–608.

[3] Ozturk, C., Y. Zhang, W. Trappe, and M. Ott, (2004). "Source-Location Privacy for Networks of Energy-Constrained Sensors" Proceedings of the Second IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems (WSTFEUS'04), Vienna, Austria, pp.68–72.

[4] Westhoff, D., J. Girao and M. Archarya, (2006). "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation" IEEE Transactions on Mobile Computing, 5, 10, pp.1417–1431.