International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Advanced Security Mechanism in Wireless Sensor Network Using Watchdog and SAFEQ Mechanism

Gajendra Singh[1], Monali V. Ghode[2]

[1]HOD, CSE Department of Computer Science and Engineering, Sri Satya Sai Institute of Science & Technology, Sehore, M.P, India

[2]Department of Computer Science and Engineering, Sri Satya Sai Institute of Science & Technology Sehore, M.P, India

Abstract: ***In Wireless Sensor Networks, where two–tier architecture is used; the storage nodes hold the data collected by sensors acting as mediator between sink and sensors. This will help in efficient query processing in WSN. However, in reality the storage nodes are the center of attraction to attackers. Recently Chen and Liu proposed a protocol that will protect the WSN and support privacy preserving range queries. This protocol uses a novel technique for encoding data, queries and results in such a way that the whole communication is secured. In this paper we implemented a custom simulator which demonstrates the proof of concept. The empirical results revealed that the proposed security approach is effective.***

Keywords: wireless sensor network, integrity, privacy, security, SafeQ

1. Introduction

WSNs are widely used application where human presence is not required or not possible. For instance they can be deployed for earthquake prediction, building safety monitoring, environment sensing and so on. In this paper two-tier architecture is considered for WSN for effective storage & retrieval. The architecture is as shown in fig.1. The storage node gets data from sensors and it is meant for storing only. The sensor nodes are responsible to sense data from surroundings and send the data to storage node. The sink is privileged to make range queries on storage node and take the required information. This architecture is flexible and ensures efficient storage. Sensors also save power by sending data to nearest node. Sensors are also relieved from storage as storage takes place in storage node. This kind of architecture is explored in [9],[11],[12],[6]. There are commercially available known as RISE [13], and StarGate[14].

The inclusion of special storage node causes security problems in WSN. The storage node is subjected to various attacks. Therefore it is important to secure communication in the WSN that is based on two tier architecture. Chen and Liu[8] presented a security protocol that ensures data integrity in WSN. The communication between the storage and sink is encoded thus making is secure. To preserve integrity and security SafeQ propose a new data structure called neighborhood chains to generate integrity verification information so that a sink can use this information to verify whether the result of a query contains exactly the data items that satisfy the query. Prior solution to this problem is proposed by Sheng and Li[1] which has two[2], [3] the data and the power consumption is more which reduces the lifetime of WSN. In this paper we built a customer simulator the simulates the sensor nodes, storage node and sink with the secure data transfer mechanisms. The simulated results encouraging and the security mechanisms are reliable.

Privacy- and integrity- preserving range queries [1] in WSN have drawn people attention recently, a scheme to preserve the privacy and integrity of range queries in sensor network. In a SafeQ protected two-tiered sensor network, compromising a storage node does not allow the attacker to obtain the actual values of sensor collected data and sink issued queries. The correctness of this claim is based on the fact that the hash functions and encryption algorithms used in SafeQ are secure. For our scheme using neighborhood chains, the correctness of this claim is based on the following three properties that and should satisfy for a query. First, items in form a chain. Excluding any item in the middle or changing any item violates the chaining property. Second, the first item in contains the value of its left neighbor, which should be out of the range query on the smaller end. Third, the last item in contains the value of its right neighbor, which should be out of the range query on the larger end. The remainder of this paper is structured as follows. Section 2 presents review of literature. Section 3 presents proposed security mechanisms. Section 4 presents simulator details. Section 5 provides experimental results while the section 6 conclude the paper.

2. Proposed System Model Security

We consider the two tier architecture for modeling the system and illustrate the mechanism to solve security problems in two tier architecture. Two-tier Architecture actually separates the layers. The sensors do not directly communicate with the sink. There is storage node which is specially meant for storing the data collected from sensor nodes. This adds flexibility to the network. The sink can make range queries on the storage node. However, this network causes security problems when storage node is compromised. Security attacks are made on storage node.

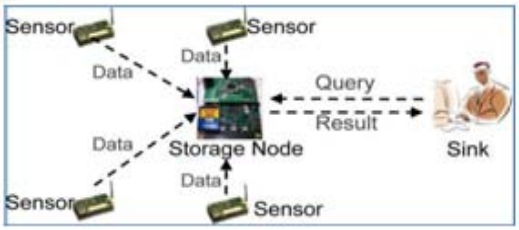

Figure 1: Architecture of two-tiered sensor networks

Fig.1 The typical Two – Tier Architecture represents, there are three different nodes involved in the architecture. They are the sensor nodes, storage node and sink. The sensor nodes are responsible to sense data from their surroundings and send the collected at a to storage node. The storage node cannot sense data. However, it can only store data. This data is queried by sink. The sink is having access to storage node and can obtain data required.

2.1 Threat Model

The sensor and sink involved in two tier architecture of WSN are assumed to be trusted. They do not cause any security problems to the network as per our assumption. When the storage node is compromised the data will be lost. We focus on protecting the storage node from malicious attacks. The proposed solution ensures data and query privacy, and data integrity.

2.2 Security Model

The security mechanism we have implemented is influenced by the approach proposed by Chen and Liu. A secret key is associated with every sensor in the WSN. Each sensor shares it with the sink. The data sensed by the sensor is encrypted using the secret key which is shared with sink. The encrypted data and associated information is sent to storage node. The protocol we implemented takes care of secure communication among the three parties such as sensor node, storage node and sink. When the sink makes query, the storage node involves in the security mechanism and finally sends requested data to sink after authenticating the sink. The sink will be able to decrypt the data with the shared key of the sensor from which the data has been collected.

3. Simulator

We used Omnet++ simulator and C++ programming language which models a network among the storage node, sensors and sink. The environment used for development includes a PC with 2GB RAM, Core 2 Dual processor running Windows 7 OS OMNeT++ IDE based on the Eclipse platform. MiXiM is an OMNeT++ modeling framework is used to model the sensor, storage node and sink with Graphical User Interface (GUI). The Four representations are presented here. Fig. 2 shows a typical sensor node which can send data to storage node.

As can be seen in fig. 2, the GUI encapsulates the sensor node. It simulates sensor node behavior. The data it senses is sent to storage node. The communication between the storage node and sensor nodes is for data transfer only. The sensor nodes do not send data directly to sink.

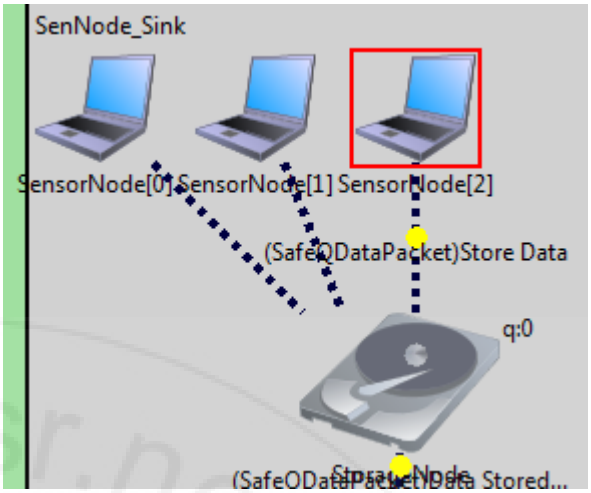

Figure 2: A typical sensor node representation

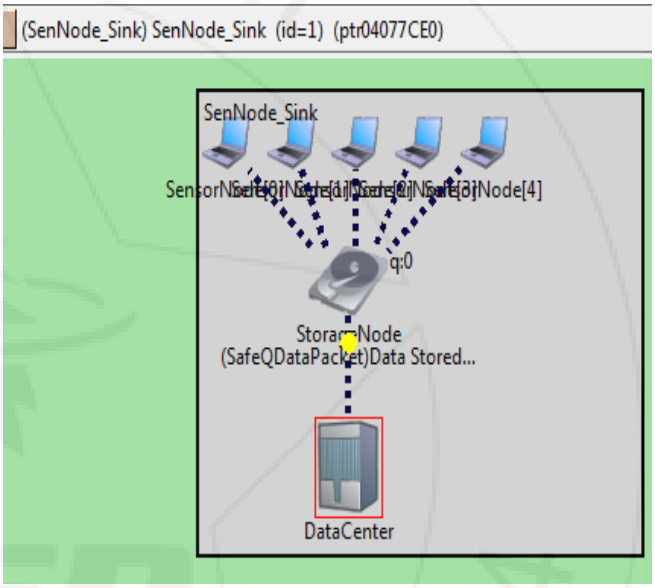

Figure 3: A typical storage node representation

As can be seen in fig. 3, the GUI encapsulates the storage node. It simulates storage node behavior. The data sent by sensor nodes is stored here. In turn it communicates with the sink. The sign takes required data from the storage node as per the two-tier architecture illustrated in fig. 1.

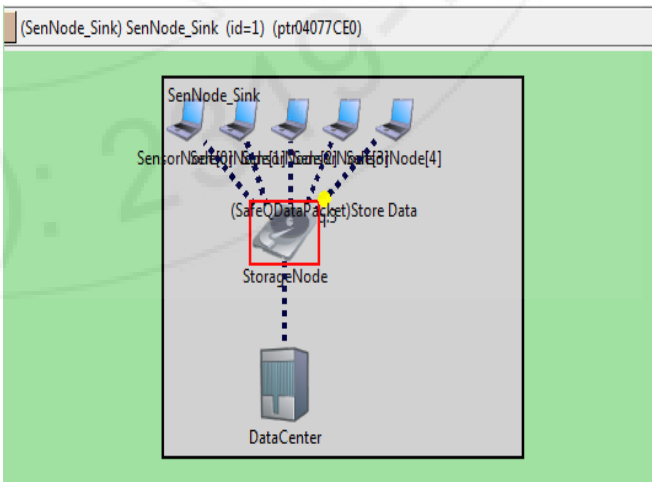

Figure 4: A typical Sink node representation

As can be seen in fig. 4, it encapsulates the sink node behavior. It is responsible to collect data from storage node as and when required. In fact it can make privacy and integrity preserving range queries to storage node to obtain required information.

4. Experimental Results

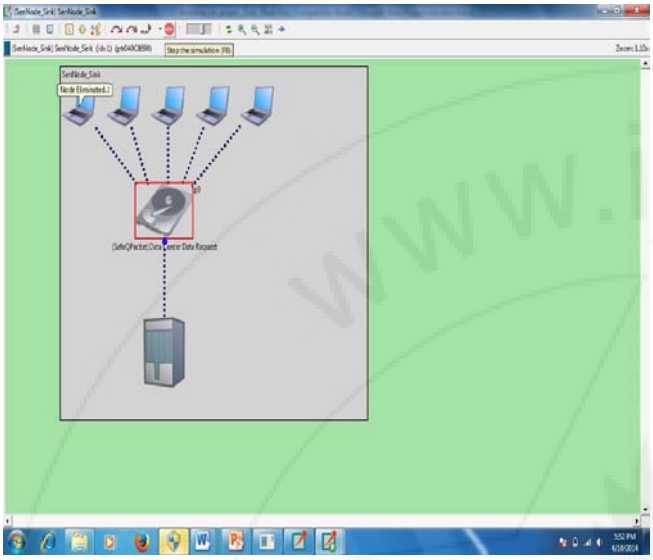

Figure 5: Fake Data representation

Figure 5: shows SafeQ detects attack successfully & eliminates nodes which sends fake data.

5. Conclusion

In WSN two tier architecture causes security attacks as the data is stored in storage node. The storage node is vulnerable as the attackers make exclusive attacks on the storage node only. Therefore it is inevitable to have a robust security mechanism that can prevent the security problems in WSN that uses two tier architecture. We implement a novel and efficient protocol proposed by Chen and Liu [1]. The protocol ensures encoded communication among the storage node and sinks to ensure data integrity. Unlike prior art, SafeQ prevents a compromised storage node from obtaining a reasonable estimation on the actual values of sensor collected data items and sink issued queries. We also build a custom simulator of WSN where the sensor, storage node and sink are simulated with their respective behavior.

We applied the protocol in order to test the network. The experimental results revealed that the proposed security mechanism is robust to attacks.

In two-tiered Wireless Sensor Network, We applied the SafeQ protocol in order to test the network in Integrity & Privacy preserving manner which will effectively & securely transfer data. Thus simulated results revealed that the proposed security mechanism is robust to attacks.

6. Future Scope

We can extend this Security Mechanism for Homogeneous & Heterogeneous WSN.

References

[1] Fei Chen and Alex X. Liu, “Privacy – and Integrity – Preserving Range Queries in Sensor Networks,” IEEE/ACM TRANSACTIONS ON NETWORKING, vol. 20, NO.6, DECEMBER 2012.
[2] Fei Chen and Alex X. Liu, “SafeQ: Secure and Efficient Query Processing in Sensor Networks,” at IEEE INFOCOM, 2010.
[3] Hero Modares, Rosli Salleh and Amirhossein Moravejosharieh, “Overview of Security Issues in Wireless Sensor Networks,” in Third International Conference on Computational Intelligence, Modelling and Simulation, 2011.
[4] Youngho Cho, Gang Qu and Yuanming Wu , “Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks,” in IEEE CS Security and Privacy Workshops, 2012.
[5] M. Kallahalla, E Riedel, R Swaminathan, Q. Wang and K. Fu, “Plutus: Scalable Secure file sharing on untrusted Storage,” in Proc. FAST, 2013, pp.29-42.
[6] Sheng and Q. Li, *“Verifiable privacy-preserving range query in two tiered sensor networks,”* in *Proc. IEEE INFOCOM*, 2008, pp. 46-50.
[7] Yong-Sik Choi, Young- Jun Jeon and Sang- Hyun Park, “A study on sensor nodes attestation protocol in a wireless sensor network,” ICACT, Feb 2010, pp.574-579.
[8] Xuhui Chen and Peiquang Yu, “Research on Hierarchical Mobile Wireless Sensor Network Architecture with Mobile Sensor nodes,” IEEE BMEI, 2010, pp. 2863-2867.
[9] P. Desnoyers, D. Ganesan, H. Li and P. Shenoy, “Presto: A Predictive storage architecture for sensor networks,” in Proc. HotOS, 2005, p.23
[10] J. Shi, R. Zhang, and Y. Zhang, “Secure range queries in tiered sensor networks,” in Proc. IEEE INFOCOM, 2009, pp. 945-953.
[11] D. Zeinalipour-Yazti, S. Lin, V. Kalogeraki, D. Gunopulos, and W. A.Najjar, “Microhash: An efficient index structure for flash-based sensordevices,” in Proc. FAST, 2005, pp. 31–44.
[12] B. Sheng, Q. Li, and W. Mao, “Data storage placement in sensor networks,” in Proc. ACM MobiHoc, 2006, pp. 344–355.
[13] W. A. Najjar, A. Banerjee, and A. Mitra, “RISE: More powerful, storage high 2005[Online]. Available: http://www.cs.ucr.edu/~rise.
[14] Xbow, “Stargate gateway (spb400),” 2011 [Online]. Available: