International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Industrial Automation and Computing (ICIAC- 12th & 13th April 2014)

RESEARCH ARTICLE OPEN ACCESS

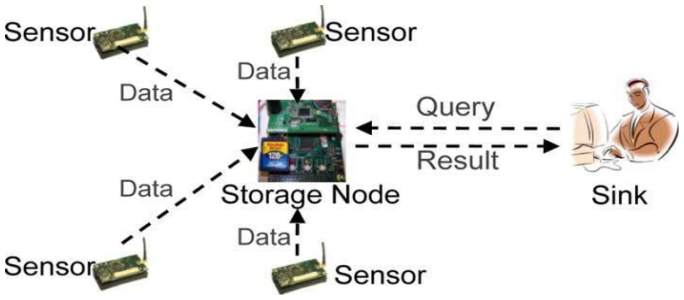
Advanced Security Mechnism In Wireless SensorNetwork-Review

Ms. Bharati A. Karare, Prof. Vaidehi Baporikar
Yeshwantrao Chavan College of Engineering, Nagpur,India
Email: bharatikarare@gmail.com, vaidehi.ycce2008@gmail.com

ABSTRACT
Wireless Sensor Network is a wired and wireless network, which consists of several sensor nodes deployed in a certain field. Storage node is located at center in two tiered sensor network, acts asa intermediate tier between the various sensors for storing data and a sink for processing queries, that has been widely adopted because of the strong capacity of power and storage for sensors as well as the efficiency of query processing. In this paper, we provide the security mechanism to Wireless Sensor Network with SafeQ protocol. SafeQ protocol prevents attackers from gaining information from both sensor collected data and sink issued queries. SafeQ also allows a sink to detect compromised storage nodes when they misbehave. In SafeQ protocol, the privacy is to be maintained by the technique of encoding both data & query without knowing their actual value & integrity is maintained by the technique of neighborhood chaining that checks whether the exactly the data items satisfied the result of the query contains

Keywords – *wireless sensor network; integrity; privacy; security; SafeQ*

In wireless sensor networks, tiny sensor nodes are spread heterogeneously. A wireless sensor network refers to a group of spacially dispersed and dedicated sensors for monitoring & recording the physical conditions of environment&organizing the collected data at a central location.Wireless sensor networks (WSN) have been widely applied to various fields like environmental conditions such as sound, pollution levels, temperature, humidity, pressure, wind speed direction, earthquake prediction etc., military measurement to the daily application fields such as fire monitoring. In this paper we consider the two-tiered sensor network architecture in which storage node acts as intermediate node between the various Sensors and sink node, storage node gather data from nearby sensors and answers queries from the sink of the network and has been widely adopted because of the strong capacity of power and storage saving for sensors as well as the efficiency of queryprocessing.



"Fig.1: Architecture of two-tiered sensor networks"

The objective of this paper is to provide security mechanism in wireless sensor network on condition that Privacy and Integrity is maintained in WSN. To prevent system from outside and inside attackers by gaining information from both sensor collected data and sink issued queries or any modification of data.Privacy and integrity is provided by SafeQ Protocol for handling range queries in two-tiered sensor networks. So that Implementation of SafeQ is also the objective of this paper. To preserve integrity, and security SafeQ propose two schemes one using Merkle hash trees and another using 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. To maintain the security of the network we have discussed mechanism a Watchdog that is a kind of behavior monitoring mechanism which is the base of many trust systems in ad hoc and wireless sensor networks. Watchdog is able to protect against a wide range of attacks and memory efficiency.

The basic issue in the two –tiered architecture is that what type of mechanism is use to secure and integrate the network?

Two-tiered sensor network is used, in that Storage nodes serve as intermediate tier. As sensors are memory limiting devices, Storage node is responsible for collecting data from near sensors and an answer queries from the sink of the network. Having more & important information stored on storage nodes, it make attractive to attacker .From storage nodes attacker may obtain sensitive data, may return forged data for a query or may not include all data items that satisfy the query.

Sensor networks edge closer towards widespread deployment, security issues become a

central concern. Up till now all the work that has been presented mainly focused on the feasibility and useful of the sensor networks. Despite of these work it is necessary to provide the security to the sensor network because these sensor measure environmental parameters and control air conditioning and lighting systems. The important question arises, if third parties can read or tamper with sensor data. In the future these wireless sensor networks will be used for most important system like for emergency and life – critical system and there these questions of security becomes foremost.

The security properties can be classified as below:[3]

Data confidentiality in the sensor network, the data should not be leak sensor reading to the neighboring network. The best solution is to encrypt the data using the secret key.

Data Integrity is necessary to ensure the receiver that the received data is not altered in transit.

Data Authentication is while injecting messages, for receiver it is need to make sure that data used in decision-making process originates from correct source. In two-party communication case, data authentication can be achieved through a purely symmetric mechanism. But the sensors need an authenticated broadcast mechanism and hence we need to construct an asymmetric mechanism from symmetric.

Wireless sensor networks are composed of large number of tiny sensor nodes, running separately, and in various cases, with none access to renewable energy resources. In addition, security being fundamental to the acceptance and employ of sensor networks for numerous applications; caused by resource restriction some of WSN applications work without security which decreased Quality of Service. Over the period many security mechanisms were proposed and implemented but still there is need to improve security mechanism with which wireless sensor network can achieve the highest privacy and can also improve the Quality of Service(QoS) in wireless sensor network.

I. Overview Of Security Mechanism In Wireless Sensor Network

The privacy, integrity and security also affect the Quality of service in Wireless Sensor Network. Quality of Service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. QoS is sometimes used as a quality measure, with many alternative definitions, rather than referring to the ability to reserve resources. Quality of service sometimes refers to the level of quality of service, i.e. the guaranteed service quality. High QoS is often confused with a high level of performance or achieved service quality, for example high bit rate, low latency and low bit error probability. Quality of service in these networks can be defined based on the number of active nodes, since if we keep this number at an optimal level, we will be able to lengthen the network life. Quality of Services in relevant to Security, Integrity and privacy for Wireless Sensor Network is mainly get affected because of the following issues:-

i. Efficiency ii. Resource Consumption iii. Packet Dropping iv. Energy Depletion

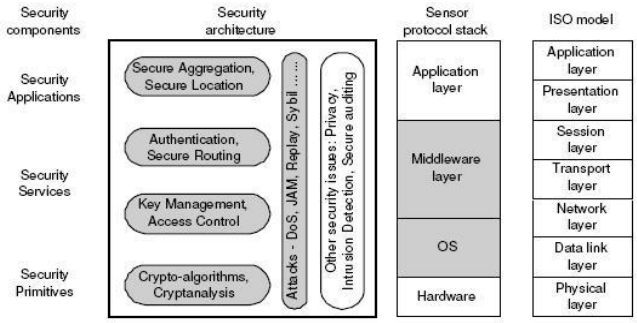


Fig.2. Security Architecture

The above fig.2. Indicating the security architecture for the Wireless sensor network, giving the overall architecture regarding the security for Wireless sensor network, having four different layers i.e. Security components, Security architectures, Sensor protocol stack, and ISO model.

II. Related Work

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, compromisinga storage node does not allow the attacker to obtain theactual 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 aresecure.For our scheme using neighborhood chains, the correctnessof this claim is based on the following three properties thatand should satisfy for a query. First, items in forma chain. Excluding any item in the middle or changing any itemviolates the chaining property. Second, the first item incontains the value of its left neighbor, which should be out of therange query on the smaller end. Third, the last item incontains the value of its right neighbor, which should be out ofthe range query on the larger end.

Verifiable privacy-preserving range query in two tiered sensor networks[6]This schemes uses the bucket partitioning idea proposed by Hacigumus et al. in for databases privacy. The basic idea is to divide the domain of data values into multiple buckets, the size of which is computed based on the

distribution of data values and the location of sensors. In each time slot, a sensor collects data items from the environment, places them to into buckets, encrypts them together in eachbucket, and then sends each encrypted bucket along with its bucked ID to a nearby storage node. For each bucket that has no data items, the sensor sends an encoding number, which can be used by the sink to verify that the bucket is empty, to a nearby storage node. When the sink wants to perform a range query, it finds the smallest set of bucket IDs that contains the range in the query and then sendthe set as the query to storage node.Upon receiving the bucket IDs, the storage node returns the corresponding encrypted data in all those buckets. The sink can then decrypt the encrypted buckets and verify the integrity using encoding numbers. The S and L scheme only considered one-dimensional data in and it can be extended to handle multidimensional data by dividing the domain of each dimension into multiple buckets.

SafeQ [2], SafeQ, a protocol that prevents attackers from gaining information from bothsensor collected data and sink issued queries. SafeQ also allows asink to detect compromised storage nodes when they misbehave.To preserve privacy, SafeQ uses a novel technique to encode bothdata and queries such that a storage node can correctly processencoded queries over encoded data without knowing their values.To preserve integrity, it uses data structure called neighborhood chains that allows a sink to verify whether theresult of a query contains exactly the data items that satisfy thequery, neighborhood chainingtechnique is an enhancement of signature aggregationand chaining technique proposed by Narasimha&Tsudik, it is much more efficient and suitablefor sensor networks because the technique directly concatenates a data item withits left neighbor without computing their digests.

Secure file systems on untrusted servers have been studied in prior work[5], which aims to design a systemwhere users can store their files on an untrusted server andthe server cannot read the content of the files. These solutionscannot solve our secure range query problem because, in suchwork, the untrusted server is not able to process queries overthe files. In contrast, processing queries in a privacy-preservingmanner at storage nodes is our main design goal for SafeQ.

Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks[4],A trust model, which is the core component of a trust mechanism, provides a quantitative way to evaluate the trustworthiness of sensor nodes. The trust evaluation is normally conducted by watchdog nodes, which monitor andcollect other sensors' behavior information. Most existing works mainly focus on the design of the trust models and howthese models can be used to defend against certain insider attacks. However, these studies are empirical with the implicitassumption that the trust models are secure and reliable. In this, we discuss several security vulnerabilities thatwatchdog and trust mechanisms have, examine how inside attackers can exploit these security holes, and finally proposedefending approaches that can mitigate the weaknesses of trust mechanism and watchdog.

Overview of Security Issues in Wireless Sensor Networks[3] focus on security of Wireless Sensor Networks (WSN) are generally set up for gathering records from insecure environment. Nearly all security protocols for WSN believe that the opponent can achieve entirely control over a sensor nodeby way of direct physical access. Different types of attacks are classified like active attacks for instances. For instance Wormhole attacks, Byzantine attacks, DDos attacks and routing attacks, are active attacks. This paper cover different types of threat and there counter measures like Eavesdropping Session, DoS Protection of network specific data link network ID, etc. Physical protection and inspection of network. Selective forwarding can be avoided by Regular network monitoring using Source Routing. Sybil Resetting of device and changing of session keys.Traffic Analysis- Sending of dummy packet in quite hours: and regular monitoring WSN network.

Research on Hierarchical Mobile Wireless Sensor Network Architecture with Mobile Sensor Nodes [8], In traditional wireless sensor networks, the users, the sink nodes and sensor nodes are considered to be static, and networks are organized by the form of single-layer planar, which can not adapt to the application of the sensor nodes with mobility. This article starts from the network architecture, introduces the architecture of traditional wireless sensor network, and takes account of the application scenario of mobile sensor nodes. Thus propose architecture of wireless sensor network with mobile sensor nodes. The architecture is dividedinto high-end node layer and low-end node layer. The high-end nodes are responsible for the data routing, and the low-end nodes are responsible for sensing and reporting data so that the mobile sensor nodes can be freed from the complicated routing calculation and implementation, and improve the network performance effectively.

A study on sensor nodes attestation protocol in a Wireless Sensor Network [7], suggests an inter-connective protocol for a sensor node that is suitable for a wireless sensor network. This protocol is able to earlier detect a node that was damaged by a neighbor node in a sensor network environment without a reliable sensor node. This protocol is for safe authentication for the sensor node. Existing research has focused on interconnective authentication for sensor nodes and the BS instead of inter-connective

authentication between sensor nodes.Therefore, when a sensor node is captured and viciously modified, and problems result in the network environment, they can be checked. The existing attestation method uses a method that proves the code of sensor node through data collective characteristics for the sensor network. In other words, theverifier regards a damaged node when there is a difference after he or she has compared the content of memory in his or her own targeted node with those of actual memory in the current targeted node.

III. Review Of Existing Security Mechanism In Wireless Sensor Networks

A) S& L Shceme

This scheme allows attackers to obtain a reasonable estimation on both sensor collected data and sink issued queries. The power consumption and storage space for both sensor and storage node grow exponentially with the number of dimensions of collected data.

B) SafeQ protocol in WSN

Privacy and Integrity are maintained by the SafeQ protocol.SafeQ protocol prevents attackers from gaining information from both sensor collected data and sink issued queries by encrypting the data and then decrypt later as required .

But the main disadvantage is this protocol is that it does not authenticate the sender. SafeQ also allows a sink to detect compromised storage nodes when they misbehave, but it does not ensure that whether data is coming from genuine sender or attacker.

C) Secure file system on un-trusted servers

The un-trusted server is not able to process the queries over the files. Also un-trusted server will not protect the network from different attacks and network can work maliciously.

IV. System Design

From the related work that was presented till now has only focused on the making sensor network feasible and useful, but not on security approach on sensor network. Despite the severe challenges of limited processing power, storage bandwidth and energy, security is important for thisdevices. Also need to work to improve the existing security mechanism it is necessary to propose the new mechanism so that third parties cannot read or tamper with sensor data and privacy can be maintained.

The main objective of this is to improve the Quality of services with more secured way in wireless sensor network on condition that Authentication, Confidentiality, Privacy, Integrity and Authorization can be obtained in wireless sensor network.

SafeQ protocol is used for providing Privacy and Integrity, a novel and efficient protocol for handling range Queries in two-tiered sensor networks.

V. CONCLUSION

In this paper, we propose the mechanism which not only make thewireless sensor network useful and feasible but also secure too which is very important for the sensor network, unless that the third parties will read or tamper the data and privacy will vanish.For that SafeQ ,efficient protocol for handling range queries in two-tiered sensor networks is effectively works. In which, to maintain privacy the technique of processing encoded queries over encoded data without knowing their actual values is used and for integritySafeQ uses the techniques like neighborhood chaining.

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.