IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 84-88
www.iosrjournals.org

PRIVACY, INTEGRITY AND SECURITY IN WIRELESS SENSOR NETWORKS: A REVIEW

Ajay Karare[1], Prof. Shrikant Sonekar[2]
[1]Student, Computer Science and Engineering, JD college of Engineering/ RTMNU, Nagpur, India
[2] Professor, Computer Science and Engineering, JD college of Engineering/ RTMNU, Nagpur, India

ABSTRACT : *The architecture of two-tiered sensor networks, consist of three types of nodes: Sensor, Storage node and a sink, where storage nodes serve as an middle layer between sensors and a sink for storing data and for processing queries, this has been widely used and adopted because of the power and storage saving benefits for sensors as well as the efficiency of query processing. In this paper, we have discussed about the different mechanisms and algorithms through which the security and integrity has been provided to the Wireless Sensor Networks, and also discussed about the drawbacks in the existing system, along with the additional mechanism to provide the Privacy to the network. To preserve the Privacy and Integrity we have mainly considered a SafeQ protocol that 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. To preserve privacy, SafeQ uses a novel technique to encode both data and queries such that a storage node can correctly process encoded queries over encoded data without knowing their values. 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.*

Keywords *-Integrity, privacy, Security, sensor networks, SafeQ, Watchdog, Merkle hash trees.*

I. INTRODUCTION

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. The increased adoption of wireless sensors across industry is due, like most industrial technologies, to solid, practical reasons. Chief among these reasons is ease of implementation (no long cable runs), ability to operate in harsh environments, easy troubleshooting and repair, and high levels of performance.

If you've been following the adoption of wireless sensor networks in industry at any level, you're bound to be aware of their prevalence in the oil and gas and water/wastewater industries—especially for use in tank farm and wellhead monitoring, where traditional wired communication is simply too costly when compared to wireless. Stories of wireless sensor successes in these applications abound.

Over The fundamental problem for a two-tired sensor network [2] is the following: How can we design the storage scheme and the query protocol in a privacy- and integrity-preserving manner?

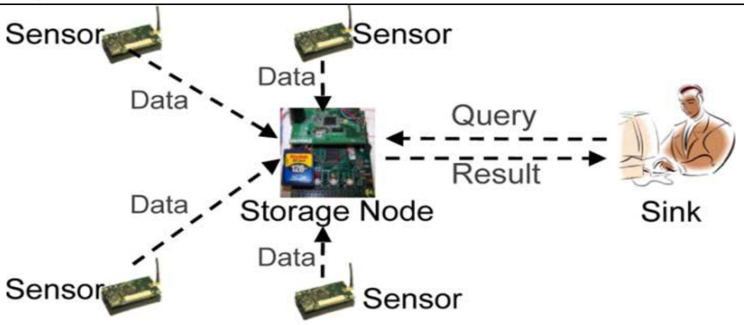

Fig.1. Architecture of two-tired sensor networks.

A satisfactory solution to this problem should meet the following two requirements.
1) **Data and query privacy:** Data privacy means that a storage node cannot know the actual values of sensor collected data. This ensures that an attacker cannot understand the data stored on a compromised storage node. Query privacy means that a storage node cannot know the actual value of sink issued queries. This ensures that an attacker cannot understand, or deduce useful information from, the queries that a compromised storage node receives.
2) **Data integrity:** If a query result that a storage node sends to the sink includes forged data or excludes legitimate data, the query result is guaranteed to be detected by the sink as invalid. Besides these two hard requirements, a desirable solution should have low power and space consumption because these wireless devices have limited resources.

The architecture of two-tiered sensor networks, where storage nodes serve as an intermediate tier between sensors and a sink for storing data and processing queries, has been widely adopted because of the benefits of power and storage saving for sensors as well as the efficiency of query processing. However, the importance of storage nodes also makes them attractive to attackers. Sensor networks edge closer towards widespread deployment, security issues become a central concern. All the work that was presented till now has focused on making sensor networks feasible and useful, and has not concentrated on security.

Despite the severe challenges of limited processing power, storage bandwidth and energy, security is important for these devices. These sensors measure environmental parameters and control air-conditioning and lighting systems. Serious privacy questions arise, if third parties can read or tamper with sensor data. In the future these wireless sensor networks will be used for emergency and life-critical systems and there these questions of security becomes foremost. The limited energy supplies create tensions for security: on one hand, security needs to limit its consumption of processing power, on the other hand, limited supply limits key life time (battery replacement reinitializes devices and zero out the keys).

The aforementioned constraints make the current secure algorithms impractical. For example, the working memory of a sensor node is even insufficient to hold the variables required by asymmetric cryptographic algorithms like RSA It is found that purely symmetric cryptographic primitives (where both parties share a common key) are more suitable for their source constrained sensor networks. The security properties required by sensor networks can be classified as below:

Data Confidentiality: A sensor network should not leak sensor reading to the neighboring networks. The standard solution is to encrypt the data with a secret key.

Data Authentication: An adversary can inject messages, so the receiver needs to make sure that the 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 primitives.

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

Data Freshness: Given that all sensor networks stream some form of time vary in measurements, it is not enough to guarantee confidentiality and authentication; we must make sure that each message is fresh. Data freshness implies that the data is recent and that no adversary replayed old messages.

The possible two types of freshness are: weak freshness, which provides partial message order but carries no delay information and strong freshness, which provides a total order on a request-response pair and allows for delay estimation. Weak freshness is enough for sensor measurements, while strong freshness is useful for time synchronization.

Despite the severe challenges of limited processing power, storage bandwidth and energy, security is important for these devices, serious privacy questions arise, if third parties can read or tamper with sensor data and if security is not maintained in wireless sensor network this security issue is also affect the Quality Of Service (QoS) of the wireless sensor network. Over the period many security mechanisms were proposed and implemented but still not having any reliable security mechanism with which wireless sensor network can become more secure, integrated and can achieve the highest privacy and can also improve the Quality of Services (QoS) in Wireless Sensor Network.

II. 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

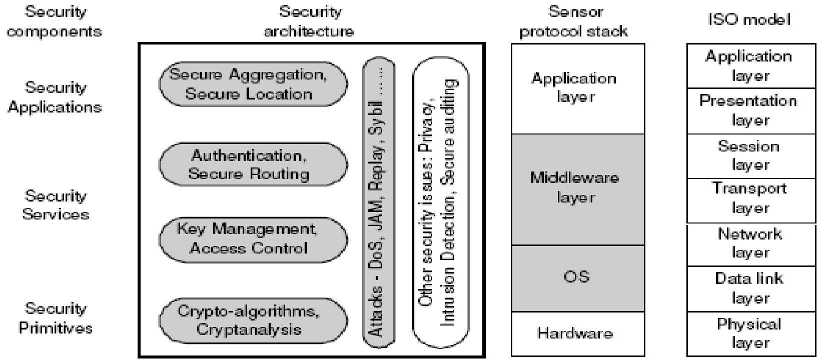

Fig.2. Security Architecture

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.

III. SOME PROJECTS AND RELATED WORK

Privacy- and integrity-preserving range queries[2] in WSNs have drawn people's attention recently, a scheme to preserve the privacy and integrity of range queries in sensor networks. This scheme uses the bucket-partitioning idea proposed by Hacigumus et al. in for database 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 into buckets, encrypts them together in each bucket, and then sends each encrypted bucket along with its bucket 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 sends the set as the query to storage nodes. 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&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, [1] a protocol that 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. To preserve *privacy*, SafeQ uses a novel technique to encode both data and queries such that a storage node can correctly process encoded queries over encoded data without knowing their values. To preserve *integrity*, SAFEQ algorithm proposed 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 improve *performance*, they propose an optimization technique using Bloom filters to reduce the communication cost between sensors and storage nodes.

Secure file systems on untrusted servers have been studied in prior work [4], which aims to design a system where users can store their files on an untrusted server and the server cannot read the content of the files. These solutions cannot solve our secure range query problem because, in such work, the untrusted server is not able to process queries over the files. In contrast, processing queries in a privacy-preserving manner at storage nodes is our main design goal for SafeQ.A trust model, which is the core component of a trust mechanism [4], provides a quantitative way to evaluate the trustworthiness of sensor nodes.

The watchdog technique [5] permits detecting misbehaving nodes. When a node forwards a packet, the watchdog set within the node ensures that the next node forwards a packet; the watchdog set within the node ensures that the next node in the path forwards the packet. The watchdogs will this by listening to all nodes at intervals transmission range promiscuously. If the node does not forward the packet, then it is considered as malicious node. In [5], they determined whether the node exhibits a malicious behavior, the watchdog counts all packets received from its neighbors and the packets should be forwarded. A neighbor trust level can be defined as the ratio between the received packets for forwarding and those effectively forwarded by the neighbor node. Watchdog employs identifier based checking of use-after-free errors almost entirely in hardware, relying on the software run time only to provide information about the memory allocations and deallocations. As pointers can be resident in any register, conceptually watchdog extends each register with a as certain if the identifier associate with the pointer being referenced is this still valid.

IV. DRAWBACKS OF EXISTING SECURITY MECHANISM IN WSN

4.1 Drawbacks of SafeQ protocol in WSN

SafeQ is a protocol that prevents attackers from gaining information from both sensor collected data and sink issued queries by encrypting the data and then decrypt later as required, i.e. privacy and integrity are maintained.

But main disadvantage in this protocol is that it does not authenticate the sender.

1. 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.

4.2 Drawbacks of “S and L Scheme”

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

4.3 Secure File system on untrusted Servers

1. The untrusted server is not able to process the queries over the files.

2. Also untrusted server will not protect the network from different attacks and network can work maliciously.

V. RESEARCH METHODOLOGY.

Sensor networks edge closer towards widespread deployment, security issues become a central concern. All the work that was presented till now has focused on making sensor networks feasible and useful, and has not concentrated on security. Despite the severe challenges of limited processing power, storage bandwidth and energy, security is important for these devices. These sensors measure environmental parameters and control air-conditioning and lighting systems. Serious privacy questions arise, if third parties can read or tamper with sensor data. In the future these wireless sensor networks will be used for emergency and life-critical systems and there these questions of security becomes foremost.

The limited energy supplies create tensions for security: on one hand, security needs to limit its consumption of processing power, on the other hand, limited supply limits key life time (battery replacement reinitializes devices and zero out the keys). The main objective of this is to improve the Quality of Services in wireless sensor network on condition that Authentication, authorization, Confidentiality, Privacy and Integrity is maintained in WSN. For this,

1. System uses digital signature for strong authentication.
2. Data Confidentiality using Asymmetric encryption.
3. Privacy and integrity is provided by SafeQ Protocol, a novel and efficient protocol for handling range queries in two-tiered sensor networks. Finally,
4. An extended watchdog mechanism besides the next-hop, node with extended watchdog will monitor all its neighbors' behavior on the base of information collected from MAC layer.

VI. CONCLUSION

The future has been predicted when wireless sensor Network would be used everywhere. In fact Wireless Sensor Network already has been implanted in various areas. The impact of these networks would be considerable and cover many aspects of daily life. The applications will not only lead to convenience but also lead to far reaching implications. Security issues related to WSN include privacy, security and integrity. Also trade-offs between security, privacy and other issues with services have to be handled carefully. So it has become the utmost necessity to raise and address the issues related to security in Wireless Sensor Network. In this paper we have discussed about different security issue in WSN and different existing mechanisms to resolve these security issues and have discussed about the limitations of existing mechanisms, and we have proposed new technology to overcome the drawbacks in the existing system, by using the SafeQ and Watchdog Mechanism Where these proposed technology will surely improve the security, privacy and integrity in wireless sensor network.

References

[1]The Fei Chen and Alex X. Liu,"Privacy- and Integrity-Preserving Range Queries in Sensor Networks", IEEE/ACM TRANSACTIONS ON NETWORKING , DECEMBER 2012.

[2]Sheng and Q. Li, "Verifiable privacy-preserving range query in two tiered sensor networks," in Proc. IEEE INFOCOM, 2008, pp. 46-50.

[3]Fei Chen and Alex X. Liu, "SafeQ: Secure and Efficient Query Processing in Sensor Networks," at IEEE INFOCOM 2010.

[4]M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. FAST, 2003, pp. 29–42.

[5]Youngho Cho, Gang Qu and Yuanming Wu, "Insider Threats against Trust Mechanism with Watchdog and Defending\ Approaches in Wireless Sensor Networks," in IEEE Symposium on Security and Privacy W,2011.