Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Advanced Network Security Using Multiple Secret Keys

S. T. Dhamdhere
M.E. Student, SPCOE, Dumbarwadi
Maharashtra, India

Dr. Gumaste S V
Professor, SPCOE, Dumbarwadi
Maharashtra, India

Abstract—This propose a security approach that uses secret key cryptography and key management along with re-keying support. A salient feature of proposed approach is that a secret key is embedded in the source code of every node to protect the other keys in its non-volatile memory. Even the node is captured physically; the sensitive information cannot be retrieved. The key selection protocol uses the node ID and some basic rotate and multiplication function to select the key for current data transmission. Because of this dynamic key selection, our approach identifies the replay attack, DoS attack and Sybil attack. The simulation results shows that our security mechanism efficiently controls various attacks with lower resource requirements and the network resilience against node capture is substantially improved.

Keywords: Secret key, Re-keying, Replay, DoS, Sybil, WSN

I. INTRODUCTION

Modern advancements in wireless technology have low-power, multifunctional wireless sensor nodes that seems to be smaller in size and can communicate in short distance in un-tethered environment. Collections of these wireless sensor nodes form a dynamic, multi-hop, routing network connecting each sensor node to more powerful traditional networks and processing resources. Most of the WSN should run continuously and reliably without any interruption. Hence incorporating security in wireless sensor networks is very challenging. Sensor Node consists of both volatile and non-volatile memory. In the non-volatile memory the static information such as program, node-ID, routing table, and security related data can be stored. WSNs have various types of attacks that include jamming attack [3], eavesdropping, packet replay attack, modification or spoofing of packets, node replication attack, Sybil attack, flooding attack, wormhole attack, sinkhole attack, denial-of-service (DoS) attacks, node compromise attack and injection of false messages through compromised nodes [4][5][6].

Data privacy and integrity preserving is more important in wireless sensor network architecture. In this paper, we consider a two-tiered sensor network architecture in which storage nodes collects data from nearby sensors and replay to the queries from the sink of the network. Hence storage nodes act as an intermediate tier between the sensors and the sink for storing data and processing queries. Storage Nodes are more important in sensor networks because of three reasons. First, sensors send all collected data to their nearest storage node. It cannot send the collected data to the sink through long routes .Hence sensor saves the power. Second, collected data are mainly stored on storage nodes because of sensors can be memory-limited. Third, query processing is done more effectively because the sink only communicates with storage nodes for queries.

i) Problem Statement

The fundamental problem Statement for a wireless two-tired sensor network is the following: How can we design the query protocol and the storage scheme to preserve a privacy- and integrity of data?

The following two requirements give the solution of this problem [7].

1. Data integrity: If a storage node sends an anonymous data to the sink then sink will detect the query as an invalid query.

2. Data and query privacy: Data cannot known by the storage node which ensures that attacker cannot understand the data stored on compromised storage node. Query privacy is defined as a storage node cannot know the actual value of sink issued queries which ensure that an attacker cannot realize useful information from, the queries received by the storage node.

ii) Existing System

SafeQ protocol which prevents attackers from gaining information from both sensors collected Data and sink issued queries. When the storage nodes will misbehave then the sink will detect it. Hence for privacy storage node should not allow the attacker which obtains the sensitive information that which will be stored in the node, as well as the queries. Those queries may treat as a confidential because such queries may leak important information from the query receiver. For integrity, to satisfy the query the sink needs to detect whether storage node includes anonymous data or does not include all the collected data that satisfy the query.

As storage nodes store data which is received from sensors and act as an important role in communication. Hence compromised storage node has significant threats to a sensor network such as the attacker can obtain sensitive data and will be added in the storage node. This storage node may not include all data items that satisfy the query in communication.

iii) Proposed system

To solve the privacy and integrity-problem, this paper will implement hash tree and digital signatures.
We summarize our own contributions as follows:
1. This paper tells about hash tree for preservation of integrity, even though hash tree deals with good digital signature technique, it can only avoid attackers it cannot remove attacker, so as a enhancement we implement a new technique of watchdog.
2.In enhancement module we implement digital signatures, a digital key is fetched to every nodes in a network, each node has to send their localization position as encrypted data using Digital signatures to the neighbours, the neighbours decrypts the data and checks the position.
3. The attacker node will not have proper digital signatures, if it sends the data to normal nodes, the normal nodes gets alerted.
4. It implement a special node called watch dog which has copy of all digital signatures, which will not involve in transmission called as a guard node.
5. If a normal nodes receives anonymous data the normal nodes gets alerted, and it alerts guard node, the watchdog will come near hacker and it will check for the signature, if the digital signatures gets varied it will delete the node from the network.

Proposed Security Approach:

This section present the overall details of security approach that ensures the following security properties:
Backward Secrecy: Even if an adversary recovered an adjacent subset of keys, it is impossible to recover the previous keys.
Privacy: Even the node is physically captured by an adversary; the secret information in the node's memory cannot be retrieved.
Data Integrity: Data Integrity ensures that the data during transmission over the network is not modified by an adversary.
Secure Management: Mechanism provide secure method for key generation as well as for re-keying which is very much necessary in defending against cryptography attacks [4].
This approach has three types of keys:
1.Data Encryption Keys (DKs): keys that are generated and shared within a group and BS.
2.Re-keying Key (RK): key that is generated and shared between a node and BS which is used during re-keying.
3.Secret Key (SK): key that is shared between a node and BS. The keys DK and RK were encrypted using SK and maintained in its volatile memory. Due to this little bit of computational overhead, even if the nodes are physically captured, the keys cannot be retrieved from its volatile memory.
The rest of this paper is organized as follows: Section 2 gives a Literature review of the related work. Section 3 describes the system model and treat model. Section 4 presents steps for system workflow and section 5 discusses conclusion.

II. LITERATURE REVIEW

A. Privacy and Integrity Preserving in WSNs

Shang and Li [1] proposed a solution of preserving the privacy and integrity of range queries in sensor networks called as S &L scheme. This scheme uses the bucket-partitioning scheme proposed by *Hacigumus et al.* to preserve for database privacy. In bucket partitioning data values are divided into multiple buckets. Size is calculated as distribution of data values and the location of sensors. This sensor collects data items, places these data items into buckets, encrypts these items together in each bucket, and then sends each encrypted bucket with bucket ID to a nearby storage node. When sink set of bucket IDs, then perform a range query, first it will search the smallest sends the query to storage nodes. The storage node will encrypt data in all those buckets. The sink performs encryption and decryption of buckets and verifies the integrity.

These scheme has two main drawbacks first, increasing the power consumption and storage space increases exponentially with dimensions of collected data. Second, the attacker can obtain sensitive data and also storage nodes may not include all data that satisfy the query in communication.
Pointed out in [2], [3], [4] preserves the data privacy and query result integrity of the range query exquisitely. These all have common drawbacks are as follows:
(1) The bucketing scheme proposed by S&L scheme may cause false positive. And query receiver would receive some useless data values.
(2) If cloud node (CN) is compromised, some data may lead to adversaries such as bucket tags.
(3) Increasing the power and space consumption increasing with the dimensions of data values.
In Safe, power and space consumption increases linearly with the number of dimensions of data items. To overcome the above drawbacks our proposed system optimizes safe protocol which consists of hash trees. In [4], It has needs to

produce many hash values by using MD5 or SHA-1 which cause large computation, communication and storage overheads. SafeQ-Bloom employs Bloom filter which represent hash values for reducing communication and storage overheads.

B. Privacy Preserving in Databases

In DAS (database-as-service) Hacigumus et al. proposed the bucket partitioning scheme for encrypted data where untrusted server will get sensitive data. *Agrawal et al.* used the bucket-partitioning scheme for investigation of range queries on numerical data. *Boneh and Waters's* scheme is expensive for sensor networks. So it cannot be used to solve privacy problem. This scheme proposed a public key system on encrypted data. *Hore et al* proposed the optimal partitioning of buckets.

III. MODELS

A. System Model

Consider two-tired sensor networks as shown in Fig.1. Architecture of two-tired sensor network consists of three types of nodes: sensors, storage nodes and a sink. Sensors are used to collect physical or environmental data, e.g., temperature which are distributed in a field. It is sensing devices with limited storage and computing power. Storage nodes are more powerful wireless devices. It has more storage capacity and computing power than sensors. Each sensor sends the information to its nearby storage node. Sink receives a query from a user and send these multiple queries to the corresponding storage nodes, which process the queries and acknowledges the query results to the sink. The Sink collects the query results from multiple storage nodes into the final answer and sends it to the original user.

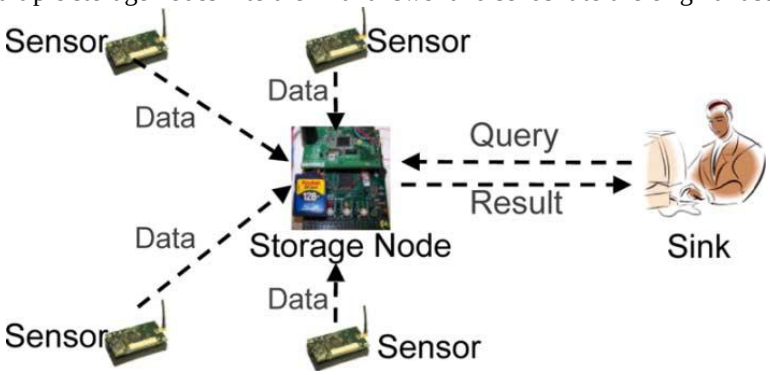

Fig. 1. Architecture of two-tired sensor networks.

***B.* Threat Model**

Sensor network is not a fully trusted. For a two-tiered sensor network, the sensors and the sink are not compromised, but the storage nodes are compromised. If a storage node is compromised then it can cause much large damage to the sensor network, i.e. the attacker will get large amount of data stored on the node. When the storage node will receives the query from the sink the compromised storage node sends a falsified result formed by including anonymous data. Therefore, compromise storage nodes will motivate the attackers. If a sensor is compromised, the attacker will get subsequent collected data of the sensor then the compromised sensor may send faulty data to its closest storage node.

IV. STEPS FOR SYSTEM WORKFLOW

1.Base file for creation of nodes and transfer of packets.

2.Topology of wireless networks with more no of nodes , transmission of packets between the nodes is done using normal AODV with attack is introduced network performance is degraded, parameters such as end to end delay, throughput, packet delivery ratio, energy spent, threshold is calculated.

3. Topology of wireless networks with more no of nodes, transmission of packets between the nodes is done by merkle hash tree and neighborhood chain schemes and attack is prevented network performance is increased, and parameters such as end to end delay, throughput, packet delivery ratio, energy spent, threshold is calculated.

4. Comparison between normal AODV and SafeQ technique is done on various parameters.

V. SECURITY ANALYSIS

This section detects various attacks such as Packet Replay attack, Sybil attack and DoS attack.

1. Replay Attack: Replay attack occurs when an attacker captures the packet at some point of time and then replays the same at later point of time without any modification.

2. Sybil Attack: In Sybil attack, any particular node claims for several identities. The Sybil node act as original node and can introduce false packets into the network and disrupt the purpose of the network.

3. DoS Attack: In DoS Attack, the attacker captures the key processing request pattern and raises these requests frequently and blocks the service availability to others.

When the base station receives the packet from the ith node, it identifies the key number to decrypt the message. If the key k cannot decrypt the received encrypted packet, it will be treated as an illegal packet. Then the base station tries to decrypt the received encrypted packet using the remaining valid keys. If the packet cannot be decrypted by

any of the remaining valid keys, then the BS identifies the packet has been corrupted. If any one of the remaining valid keys decrypts the packet, then the BS verifies the timestamp Ti. If the packet is not a fresh packet, then the BS declares that this is a replay packet. If the packet is a fresh one, then the BS declares that this is a Sybil attack and it broadcast a message to invalidate the key number of the group.

VI. CONCLUSION

It propose an efficient range query analysis for two tiered sensor networks to preserve privacy and integrity of data. To preserve a privacy and integrity, it implement a new technique of watchdog which receives an anonymous data from normal nodes then it will hack the hacker and verify the digital signature. If does not verified then it will delete the node from the network.

This approach uses one-way hash function to dynamically generate the keys that avoid transmission of key during runtime. In order to minimize the memory overhead, we have introduced grouping among nodes in the network that maintains different sets of keys. Our approach identifies the attacks such as Replay attack, Sybil attack and DoS attack. It present a mechanism by analyzing the parameters such as network availability, packet delivery and network energy on replay and DoS attacks. In proposed mechanism, scalability can be still increased by introducing the Clustering concept in order to reduce the traffic and overhead to the Base Station. This mechanism study the network parameter s such as end to end delay, throughput, packet delivery ratio, energy spent, threshold using hash tree and digital signatures to increase network performance.

REFERENCES

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

[2] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. TCC, 2007, pp. 535–554.

[3] F.Chen and A. X. Liu, "SafeQ: Secure and efficient query processing in sensor networks," in Proc. IEEE INFOCOM, 2010, pp. 1–9.

[4] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. ACNS, 2004, pp. 31–45.

[5] R. Zhang, J. Shi, and Y. Zhang, "Secure multidimensional range queries in sensor networks," in Proc. ACM MobiHoc, 2009, pp. 197–206.

[6] S. Mehrotra, and G. Tsudik, "A privacy-preserving index for range queries," in Proc. VLDB, 2004, pp. 720–731.

[7] Shi, R. Zhang, and Y. Zhang, "Secure range queries in tiered sensor networks," in Proc. IEEE INFOCOM, 2009, pp. 945–953.

