Security in Wireless Sensor Network Using Cryptographic Techniques

Dhamdhere Shubhangi T., Dr. Gumaste S. V.

Abstract: Due to lack of tamper-resistant hardware and broadcast nature of Wireless Sensor Networks (WSNs), security in sensor networks is one of the major concerns. WSNs consist of a large number of sensor nodes and a few sink nodes or Storage node are used to collect information about the state of physical world and transmit it to interested users. It used in applications such as, health monitoring, habitat monitoring, military surveillance and environment sensing. Sensor nodes have limited resources in term of processing power, battery power, and data storage. A sensor network that is not fully trusted that's why privacy is to be preserved. A security approach that use secret key cryptography and key management. To preserve the integrity, a digital key is fetched to every node in a network, each node has to send their localization position as encrypted data using digital signatures to the storage node and it decrypts that data and checks the position by using authentication. RSA algorithm with MD-5 is used for authentication. A malicious node attacks in any network to disrupt the proper functioning of the network. Such attacks may cause damage on a large scale network especially since they are difficult to detect. In this paper, results shows network parameters like end-to-end delay, energy consumption attack detection with and without watchdog security. Hence, this paper focuses on various security issues, security threats, and various types of attacks.

Keywords: Wireless Sensor Networks, Digital signature, attacks, Security.

I. INTRODUCTION

Today's cryptography is more than encryption and decryption. Authentication is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives when we sign our name to some document and for instance and, as we move to world where our decisions and agreements are communicated electronically, we need to have electronic techniques for providing authentication. Cryptography provides mechanisms for such procedures. A digital signature binds a document to the possessor of a particular key, while a digital timestamp binds a document to its creation of a particular time [4][6]. Modern advancements in wireless technology have enabled the growth of packed in, low- power, multifunctional wireless sensor nodes that look smaller in size and can communicate in short distance even 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[2]. In the battlefield surveillance application, sensor nodes could monitor the passage of vehicles and sometimes used to track the position of enemy or even safeguard the equipment. Some other critical applications like forest fire detection, the wireless sensor networks are designed for early detection of forest fires [1]. The basic task of sensor networks is to sense the events, collect data and send it to their requested destination. Sensor Networks applications such as military application has mission-critical tasks and so it is clear that security requirement to be taken into account during the design time itself. Furthermore, most of the network should run continuously and reliably without any interruption. Hence incorporating security in wireless sensor networks is very challenging. It has various types of attacks that include jamming attack, 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[7].The key distribution and management are considered to be the core of secure communication. In this proposed security mechanism, the keys are not directly distributed over the network at any time. Instead, the parameters that are used to generate the keys are transmitted only during re-keying. It is significantly hard for an adversary to identify those parameters.

II. MAIN FLOW DIAGRAM

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. 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

ISSN: 2278 – 7798

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.

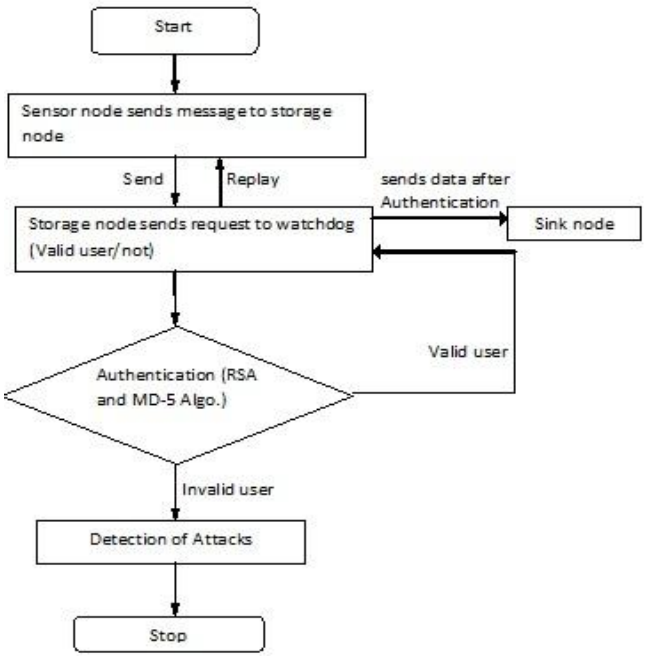


Fig No.1.1

III. RSA ALGORITHM AND IT'S MATHEMATICAL FOUNDATION

It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization .

3.1 RSA Authentication using MD-5 for Hashing

RSA can be used for Digital Signature. For Digital signature the message is first encrypted by private key of sender and encryption is done by public key of receiver. This gives confidentiality and authentication. MD5 can be used for preparing a message digest which is encrypted along with the message and sent to the receiver for verification.
The general algorithm used can be summed up as:

Sender:

1. Apply hash function to the message h(m)-MD5.
2. Choose two primes p and q, and computes n = pq.
3. Choose eA such that 1 < eA <(n) with gcd (eA, (n)) = 1.
4. Calculate dA such that eAdA 1 (mod (n)). Keep dA, p, q secret and publish (E, n).
5. Sign the message S h(m)dA (mod n). The pair (m, S) is made public.

Receiver:

1. Apply hash function to the message h(m).
2. Decrypt the signature z SeA (mod n).
3. If z = h(m), the signature is valid

3.2 Security of RSA

The security of RSA algorithm depends on the ability of the hacker to factorize numbers. New, faster and better methods for factoring numbers are constantly being devised. The Trent best for long numbers is the Number Field Sieve. Prime Numbers of a length that was unimaginable a mere decade ago are now factored easily. Obviously the longer a number is, the harder is to factor, and so the better the security of RSA. As theory and computers improve, large and large keys will have to be used. The advantage in using extremely long keys is the computational overhead involved in encryption/decryption [4]. This will only become a problem if a new factoring technique emerges that requires keys of such lengths to be used that necessary key length increases much faster than the increasing average speed of computers utilizing the RSA algorithm. RSA's future security relies solely on advances in factoring techniques.

IV. DIGITAL SIGNATURE ALGORITHM

DSA is based on Digital Signature Standard and essentially a modification in Signature Scheme. The security of the algorithm is based on problem of finding discrete logarithm of large values of prime[6].
The Digital Signature Algorithm can be summed up in three Steps:

4.1 Key Generation:

1. Choose a 160-bit prime q.
2. Choose an L-bit prime p, such that p=qz+1 for some integer z, 512 = L = 1024, and L is divisible by 64.
3. Choose h, where 1 < h < p -1 such that g = hz mod p>1. (Recall that z = (p-1)/ q)
4. Choose x by some random method, where 0 < x < q.
5. Calculate y = gx mod p.
6. Public key is (p, q, g, y). Private key is x.

4.2 Signing:

1. Generate a random per-message value k where 0 < k < q
2. Calculate r = (gk mod p) mod q
3. Calculate s = (k-1(SHA(m) + x*r)) mod q, where SHA(m) is the SHA-1 hash function applied to the message m
4. Recalculate the signature in the unlikely case that r=0 or s=0
5. The signature is (r, s)

4.3 Verifying:

1. Reject the signature if either 0< r <q or 0< s <q is not satisfied.
2. Calculate w = (s)-1 mod q
3. Calculate u1 = (SHA(m)*w) mod q
4. Calculate u2 = (r*w) mod q
5. Calculate v = ((gu1*yu2) mod p) mod q

The signature is valid if v = r

V. SECURITY ANALYSIS

Security in sensor networks is as much an important factor as performance and low energy consumption in many applications. Security in a sensor network is very challenging as WSN is not only being deployed in battlefield applications but also for surveillance, building monitoring, burglar alarms and in critical systems such as airports and hospitals. The sensor nodes are present outside the building so it must protect from the physical changes such as raining,

ISSN: 2278 – 7798

temperature etc. Since sensor networks are still a developing technology, researchers and developers agree that their efforts should be concentrated in developing and integrating security from the initial phases of sensor applications development; by doing so, they hope to provide a stronger and complete protection against illegal activities and maintain stability of the systems at the same time.

Types of security attack:

There are two types of security attack are present active attack and passive attack.

1. Active attack in which the attacker cause modification of data. There is physical damage in the network like modification of resources, alteration of data, changing traffic direction or stoppage of data to sink nodes. These attacks are easily identifiable and can stop the attackers as well as start the system recovery process.

There are four categories of active attacks are present masquerade, replay, modification of messages, and denial of service.

1. A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack

2. Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

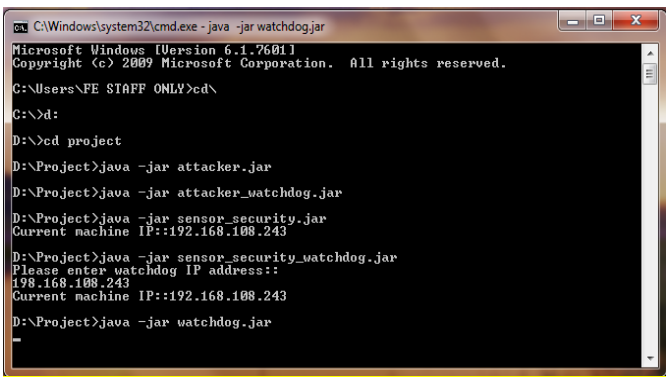
3. The messages means that some portion of a message is altered or those messages are delayed or reordered, to produce an unidentified effect is called modification attack.

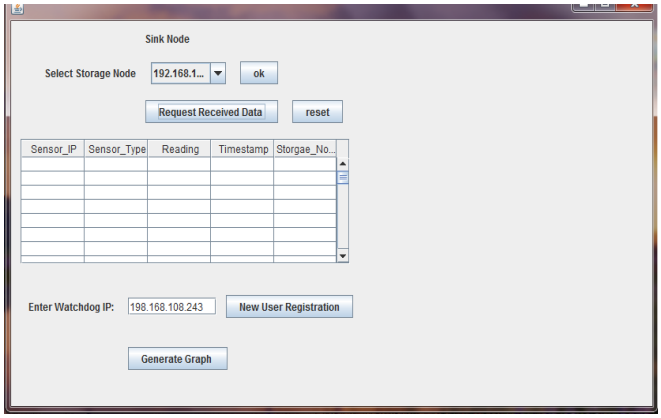
4. The denial of service will consume resource of network for unwanted operation. The denial of service prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target, as a result the entire network either by disabling the network or by overloading it with messages so as to degrade performance [7].

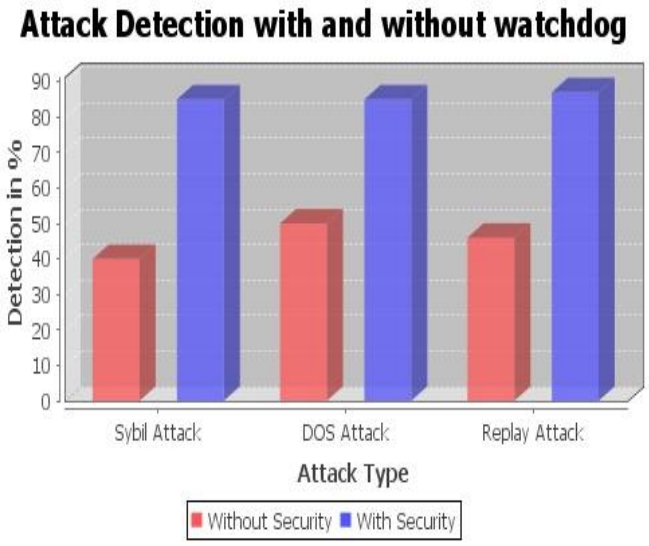
2. Passive attacks are in the nature of eavesdropping on, or monitoring of transmissions. The goal of this is to obtain information that is being transmitted [8].

RESULT AND EVALUATION

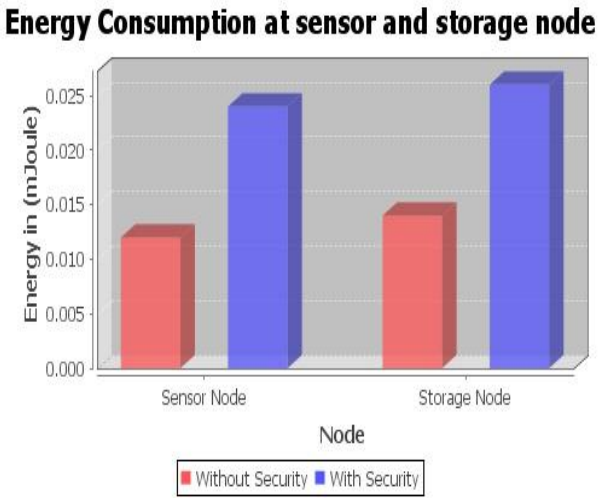
We evaluate the performance of different cryptographic schemes on the basis of metrics like throughput, end-to-end delay and energy consumption. The cryptographic security schemes had impact on the quality of service of the WSN because of limited constraints. To analyze the performance of the security schemes by varying the nodes, the metrics used to evaluate the performance are given below.







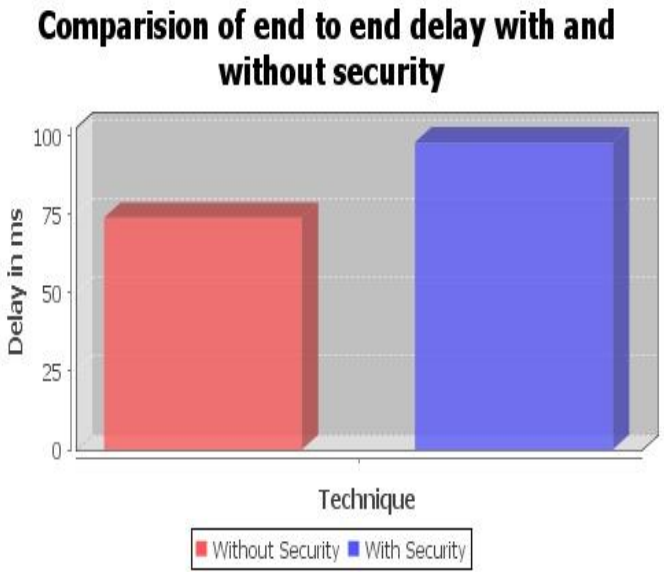
The above graph shows the variation in the throughput of watchdog and other different security schemes. In this, the throughput of watchdog security scheme is more than other security schemes.



This graph shows the variation of energy consumption of watchdog and other security schemes. In this the watchdog

ISSN: 2278 – 7798

security model consumed more energy in transreceiver modes as compared to other security schemes and it further increases with scalability.



The above graph shows the variation in the end-to-end delay of different security schemes in wireless sensor network. The watchdog security scheme has higher end-to end delay than other security schemes.

VI. CONCLUSION

Technique proposes an efficient range query analysis for two tiered sensor networks to preserve privacy and integrity of data. To preserve a privacy and integrity, it implements 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. Proposed approach identifies the attacks such as Replay attack, Sybil attack and DoS attack and also applies to sensor node. This proposed mechanism increases network performance by the study of the network parameters such as end to end delay, Energy consumption and detection of various attacks using hash tree and digital signatures.

VII. FUTURE SCOPE

Scalability can still be increased by introducing the Clustering concept in order to reduce the traffic and overhead to the Base Station.

REFERENCES

[1] Sheng and Q. Li, "Verifiable privacy-preserving range query in two-tiered sensor networks," in Proc. IEEE INFOCOM, 2008, pp. 46–50.
[2] Shi, R. Zhang, and Y. Zhang, "Secure range queries in tiered sensor networks," in Proc. IEEE INFOCOM, 2009, pp. 945–953.
[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] MJ Wiener. (1990), "Cryptanalysis of short RSA secret exponents", IEEE Transactions on Information Theory, Vol 36, No 3, pp 553-558.
[5] R Gennaro. (2000), "RSA-Based Undeniable Signatures", Journal of Cryptology, Vol 13, No. 4, pp 397-416.
[6] R Cramer, V Shoup. (2008), "Signature schemes based on the strong RSA assumption", ACM Transactions on Information and System Security, Vol 3, No 3, pp 161-185.
[7] D. Murat, and S. Youngwhan, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", World of Wireless, Mobile and Multimedia Networks, WoWMoM 2006.
[8] A. V. PRAMO, Md. Abdul Azeem, M. OM PRAKASH "Detecting the Sybil Attack in Wireless Sensor Network", International Journal of Computers & Technology, ISSN: 2277-3061 Volume 3, No. 1, AUG, 2012.

About Authors:

[1] Ms. S.T.Dhamdhere, ME student, Department of Computer Engineering, SPCOE-Dumberwadi, Otur.

[2] Dr. S. V. Gumaste, currently working as Professor and Head, Department of Computer Engineering, SPCOE-Dumberwadi, Otur. Graduated from BLDE Association's College of Engineering, Bijapur,Karnataka University, Dharwar in 1992 and completed Post-graduation in CSE from SGBAU, Amravati in 2007. Completed Ph.D (CSE) in Engineerng & Faculty at SGBAU, Amravati. Has around 22 years of Teaching Experience.

ISSN: 2278 – 7798