A Survey on Cryptography and key distribution in Wireless Sensor Network with Security Attack and Challenges

Chirag H Bhatt[1],Himanshu H Patel[2],Mr. Dushyantsinh B. Rathod[3]
Faculty Of Engineering, Shree Saraswati Education Sansthan, Kadi, India[1,3]
PG Student of Computer Engineering, GTU PG School, BISAG-Gandhinagar[2].
Chiragbhatt005@gmail.com[1], himanshupatelxyz@gmail.com[2], dushyantsinh.rathod@gmail.com[3]

***Abstract*—Wireless Sensor Network(WSN) are consists of large number of low power sensor nodes. Security in WSN is very crucial when there are Eavesdropper. There are Two Type of Cryptography method. Symmetric which use same key for both encryption and decryption. Another one is Public key cryptography in which use two different keys, public and private. Pairwise key establishment is a fundamental security service. There are several existing key management schemes have been shown for the establishment of pairwise key between sensor nodes. Here there are two key pools in which one key pool are the hash value of the keys in another key pool. Present scheme provide better resilience against node capture attack. Different types of Security attack happen in WSN like jamming, Tampering, collision, hello flood etc. the challenges in it are Measuring confidentiality, Timing Obfuscation, Secure aggregation, Topology, Obfuscation, Scalable Trust Management Aggregation with Privacy.**

Keywords : Wireless Sensor Network, key management ,hash function ,security attack, challenges

I. INTRODUCTION

Wireless sensor network (WSN) have broad field of application such as remote monitoring, environmental sensing and target tracking. The main goal of WSN is to collect information from real world. The WSN consist of low power sensors node equipped with one or more sensors. The sensor node is useful to get the information like pressure, temperature, light, motion, sound and process the information. But when the sensor nodes are placed randomly in the hostile environment, security becomes very extremely important factor. the sensed data of sensor nodes is prone to different types of attack before reaching to the base station. The base station is only used for gathering the data from the distributed sensor nodes. Security is needed in the communication part in the network to provide the accurate data. So protect the sensed data is critical task.

II. SENSOR NETWORK COMMUNICATION ARCHITECTURE

The sensor nodes are usually moves in the sensor field. Each of the moved sensor node has the capabilities to collect data and route data back to the sink node and to the users via internet. Base station is centralized point of control within the WSN. Which extract the information from the network and disseminates control information back to the network? It also used as a Gateway to the other networks, As far as Hardware concern the base station is either laptop or a workstation.

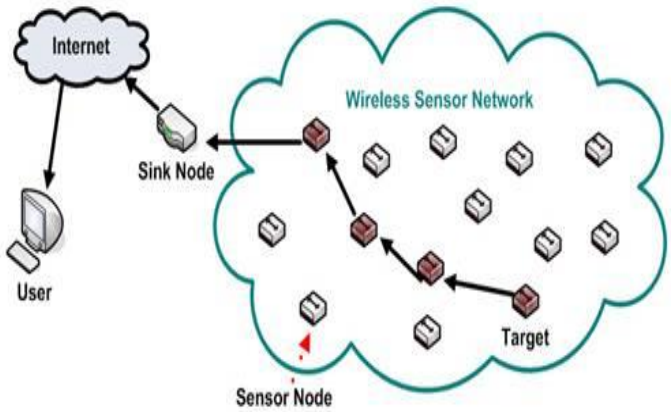

Figure 1 Network

III. SECURITY REQUIREMENT

Sensor network used for many applications where the security is the key issue. Our aim to achieve the way in which the secure communication occurs among the nodes. Here we can't use the general security communication Techniques for WSN because of resource-constraints and communication overheads involved[1].The security requirement of wireless sensor network can be classified as below.

A. Authenticity

It is an important application in sensor network. Adversary can easily inject messages, receiver need to ensure that the data used in the decision making process comes from the trusted sender. This is allowing to the sender and receiver must be sure that they are talking to the node to which they want to communicate.

B. ***Confidentiality***

Confidentiality means the guarantee that data sent on the channel will not be read or decoded by the other inappropriate node except the actual receiver. Here the message is sent on the channel in the encrypted form. It means keeping information secrete from unauthorized parties.

C. ***Integrity***

Here the data should not be modified by any adversary to the receiver. If it occurs then the receiver must verify that the data received is exactly the same as sent by the sender. for this purpose the message authentication code (MAC) is generated by the sender using some MAC key and that is sent with the encrypted message. The receiver will verify the authentication of the received message bu using the MAC key.

D. Scalability

If the network size grows than it should not be the changes of node compromise, should not increase communication overhead. It should allow nodes to be added after the network deployment.

IV. SYMMETRIC KEY CRYPTOGRYPH

Selection of a suitable security scheme is critical in wireless sensor networks (WSNs) because of the open media broadcast communication and the limited energy supply of the sensor device [1]. To achieve the security requirements, several researchers have focused on evaluating cryptographic algorithms in WSNs and proposing energy efficient ciphers. Although the transmission of data is the most energy consuming activity in a wireless sensor node, it is also important to select an energy efficient cipher that will minimize the energy consumption of the energy constrained sensor node [2].

In Symmetric encryption same key is use for both encryption and decryption of data. Algorithm used for this is easy to implement and required limited computation power for encryption and decryption .Problem is all participant node agree on same key.so this scheme is more vulnerable. And many attack like eavesdropping and capture attack is possible. Below describe the keying model of Symmetric cryptography.

Global Keying

The simplest keying model uses a single global key. Known by all nodes and used by all nodes during communication. This makes key management trivial, but comes with the cost of lower security. If an adversary compromises one node ,it undermines the security of the whole network .

Pair-Wise Keying

Using pair-wise keys, unique key is assigned to each pair of nodes. This is much more secure than a global key, but the storage overhead become very large if a node communicates with many nodes.

Group Keying

Group keying partitions the network in to group and uses a unique key for each group .All Communication within the group uses this key. This creates the possibility to trade off group size for security.

Hybrid Approaches

To allow more flexibility, these keying models can be combined by using a different keying model for different communication types. For example by using pair-wise key for node to base station communication and a global key for node to node communication.

Five popular encryption schemes is used in Symmetric key Cryptography. RC4,RC5,IDEA,SHA-1,andMD5.were evaluated on six different microprocessor ranging in word size from 8 bit (Atmel AVr) to 16 bit bit(Mitsubishi M16C) to 32 bit widths(Strong ARM,XScale) in.[3]

Two type of Cipher in Symmetric cryptography.one type of symmetric cipher is block cipher,e.g AES which transform a string of a certain length to another string of certain length.it needs an encryption function to make it possible to use this cipher on longer strings. The plain text is divided into a blocks that are encrypted one at a time. The encryption function often takes an initialization vector(IV) or nonce as input to make it more resistant to attacks. Another cipher text is stream cipher which simulates an infinitely long key and encrypts one bit or character at a time and can therefore encrypt plaintexts of any length. Because block cipher encrypt multiple bits at a time, implementations of block ciphers run faster than implementations of stream cipher.

V. PUBLIC KEY CRYPTOGRAPHY

Problem of symmetric key is how to send a key.to solve the problem public key is come. Public key cryptography was invented in seventies years. In this cryptography two key are use to encrypt and decrypt of data. any message or data encrypted with one of the keys can only be decrypted with the other key. In Two key one key is private and another is public key. private key is known by only itself node which it hold, and the second one is publicly known by each node in a given community this ensure confidentiality, integrity and authentication. Often the management of generation, distribution, renewal and publication of these keys is achieved

by a trust party called Certificate authority (CA) which composes what we call public key infrastructure (PKI)which is recognized as the most efficient and powerful tool to ensure key management in conventional networks. However PKI is omitted from the use in WSN, because of its great consumption of energy and bandwidth which are very crucial in sensor network, and all the most known solution given in literature use symmetric encryption which is more power saving.[4]

Now a day a sensor become more powerful in terms of CPU and memory power, so we can use public key cryptography in WSN.

Due to large code size, data size and power consumption used in RSA and Diffie–Hellman key.it is very insufficient for used in sensor network. In RSA for performing single security operation that execute thousand of multiplication instructions.

In RSA there is two phases, the first is the sensor to base station handshake in which the base station and a given sensor node setup a session key to secure end to end link between them, this handshake is protected and authenticated using the public key of the base station. The second phase is the use of this session key for data encryption to ensure confidentiality and ensuring the integrity of the exchanged data using the MAC joined to each packet[4].

In Public key Cryptography mostly two algorithms RSA and ECC use. The ECC is offer equal security for a far smaller key size than any other algorithm. So that it reducing processing and communication overhead. For example, RSA with 1024 bit keys (RSA-1024) provides a currently accepted level of security for many applications and is equivalent in strength to ECC with 160 bit keys (ECC-160) .To protect data beyond the year 2010, RSA Security recommends RSA-2048 as the new minimum key size which is equivalent to ECC with 224 bit keys (ECC-224)[4].

VI. OPEN RESEARCH ISSUES

Use of prepare cryptography method for sensor nodes for providing security services in WSNs. This things depends on the communication capability and computation of the sensor nodes. Now a day public key cryptography operation is popular as compare to the private key encryption.

Symmetric key cryptography is much better than Public key cryptography in terms of speed and low energy cost. But the key distribution is much harder in symmetric key cryptography

VII. PAIRWISE KEY ESTABLISHMENT SCHEME

A fundamental security service is to establish pairwise key shared between two sensor nodes, which is the basis of other security such as encryption and authentication. The main problem in the key management is to establish the secure keys between the sensor nodes. but due to the resource constraints, implementation an efficient key establishment mechanism is not a trivial task. In this scheme we define how the proposed key redistribution scheme works in details.

In our scheme there are two key pools. The keys in the first key pool are generated directly by setup server. And the keys in the second key pool are the hash value of the keys in the first key pool. here the one way property if too know the value of first key pool than using hash function you can compute the value of second key pool but vice versa not true.

Here the scheme is divided in the three phases: Setup Phase, Direct Key Establishment Phase, and Path Key Establishment Phase. The setup phase is performed to initially the sensor nodes by key distribution to them. After the nodes has been deployed, if any two nodes need to establish a pairwise key then they first go for direct key establishment. If they can successfully establish a common key, then there is no need of path key establishment. Otherwise the path key establishment start Trying to establish the pair wise key with the help of other sensor nodes[5].

A. Key Predistribution Phase

This Phase is conducted offline by a setup server before all
Sensor nodes have been deployed in a target field. the main purpose of this phase is to assign the key materials to each sensor node in the field. Using this key material the neighboring nodes could setup pairwise keys after deployment. It has the following below step.

Step1: The setup server generates w keys, which are called original keys. Then after setup server generates w new keys, which are called derived keys; it will be generated by applying the hash function to the original. There are total 2w keys from the key pool p. Here, each key in the key pool has two parts (ID,T).The T indicates the type of key. T is either 0 or 1.When T is 0 then key is original key and when T is 1 the key is derived key.

Setp2: For each sensor node, the setup server stores choose the hash function H, Which is useful to generate the derivative keys into each sensor node.

Step3: For each sensor node the setup server randomly t original keys and t derivative keys, which have distinct ID, from the key pool p and store them into each sensor node. Here we call the set of the t keys the node's key ring.

B. Shared Key Discovery Phase

After the sensor nodes have been deployed the shared key discovery phase will be applied. During this phase first the sensor node finds out with which of their neighbors the share a key. To find out the whether the node has the common ID with its neighbors, the source node disclose a list of key IDs and the type these keys to the destination.

We guess that the sensor node U and V are neighbors, whenever the sensor node U is to find or calculate the shared keys with sensor node v.it needs to Matches the key index ID. If the index Id of the key Ku in the sensor node u is the same as that of key Kv in sensor node v. They can compute the pairwise secrete key as follow, three cases as below.

Case1: The T of the key Ku is same as that of the Kv. In this case, two sensor node can use the Ku or Kv as their communication key.

Case2: The T of the key Ku=1and that of key Kv=0.In this case ,the sensor node v need to calculate H(Kv) as pairwise key and sensor node u needs no calculation and uses Kv as the pairwise key.It is obviously thet Ku=H(Kv).

Case3: The T of the key Ku=0 and that of the key Kv=1.In these case,the sensor node u need to calculate H(Ku) as the pairwise key and sensor node v needs no calculation and uses Ku as the pairwise key.It is obviously that Kv=H(Ku).

C. Path Key Establishment Phase

Once the direct key establishment fails, the pairwise key establishment occurs between two sensor nodes with the help of other sensor nodes. To establish the pairwise key with sensor node u,the sensor node v need to find a path between them such a way that the two adjacent sensor node in the path can establish a pairwise key directly .Then the sensor node U or V initiates the request to establish a pairwise key with the other sensor node using the intermediate nodes along the path.

VIII. Classification of Vulnerabilities in WSN as Active/Passive attacks

Active attack: Those attacks which attempt to alter, inject, delete or destroy the data being exchanged in the network. Intention of such an attack is to damage the network or disrupt the network operations. Example: Fabrication or masquerading attacks, message modifications, message replays and DOS attacks. Since the attacker is already part of the network, internal attacks are more dangerous and hard to found than external attacks.

Passive attack: Those attacks which attempt to learn or make use of information but do not affect the system resources. Such an attack has no intention to damage the network & network operations because it does not modify the contents of the packets. Example: Eavesdropping, Release of message contents and Traffic analysis. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. This classification on the basis of emission of an attack can further be used to categorize different attacks. Such a classification is mentioned in Table 1 where some of the common attacks are classified as Active or Passive.

Table 1 Attack and its Type

Name of Attack	Type of Attack (Active or Passive)
Worm hole, Denial of Service, Black hole, Interference & Jamming, Malicious code, Session hijacking, Impersonation, Routing attacks, DOS	Active Attacks
Eavesdropping, monitoring, Snooping, Selfish misbehavior, traffic analysis.	Passive Attacks

Table 2 Protocol Stack Based Security Vulnerabilities

Name of the layer	Countermeasures
Application Layer	Firewall
Transport Layer	Client,Puzzles, Rate Limitation
Network Layer	Authentication, monitoring
Datalink Layer	Error-correcting code ,Rate limit, Small frames
Physical Layer	Spread-Spectrum ,Priority message ,hiding, Tamper-proofing

Here in the table 3 denotes the simple TCP/IP Stack and the WSN Stack In which the Security Vulnerabilities in WSN are described. At each layer of the WSN stack which attacks are occurred are shown.

Table 3 TCP/IS stack and WSN stack

TCP/IP PROTOCOL STACK		WSN PROTOCOL STACK	SECURITY VULNERABILITIES IN WSN	

Application		Application	Repudiation, Malicious code attack
Transport		Transport	Flooding
Network		Network	Black holes, Hello Flood, Sink hole, Sybil, Selective forwarding
Data Link		Data Link	Collision, Exhaustion, Unfairness
Physical		Physical	Jamming, Tampering

1. Jamming Attack: Interferes with the radio frequencies the node are using. Only a few Jamming node can put some amount of nodes in out of order. If the neighboring background change than also jamming attack happen.
2. Tampering attack: Here the attacker will change the node it self or do some changes in the node hardware structure and also find the solution to access higher communication layers.
3. Collision Attack: Here the attacker damage the transmission so that the checksum for sender and receiver are different and packet can be disrupted[10].
4. Exhaustion Attack: Here occurs only when unnecessary retransmission of packets occurs for the late collisions.
5. Selective Forwarding: Here the attacker include his/her path of interest in data. Then it decide that some of the packets are not forward and drop of them. This attacks are much harder to detect.
6. Sinkhole Attack: It work by making a compromised node attractive to it's neighbors. Sensor network are susceptible to these attacks due to their multi hop nature and the specialized communication pattern they use.
7. Sybil Attack: This attack targets fault tolerant schemes such as distributed storage, dispersity, multipath routing and topology maintenance.
8. Wormholes: In these attacks the adversary tunnels messages received in one part of the network over a low latency link, to another part of the network where the messages are then replayed. When this attack is combine with selective forwarding and the Sybil attack it is very difficult to detect.
9. Hello Flood Attack: In many routing protocol , nodes broadcast hello messages to show their presence in network. A node receiving such a message can assume
   that the node send the message is in it's range.

IX. COUNTERMEASURES

Here show how the security Vulnerability affect the layer of the protocol stack.so we can find some solution to overcome to it and how to defense against them. below are the some techniques:

X. SECURITY CHALLENGES

Challenge 1: Measuring Confidentiality which is defined models and metrics for information privacy and security properties of sensor network protocol.

Challenge 2: Timing Obfuscation which is to identify the cost effective schemes for hiding the timing information in the sensor networks.

Challenge 3: Secure Aggregation which is to develop novel cryptographic solutions that allow aggregation of messages while ensuring adequate security.

Challenge 4: Topology Obfuscation is to hide the routing infrastructure.

Challenge 5: Scalable Trust Management is to develop lightweight key management and distribution schemes appropriate for large-scale sensor node.

Challenge 6: Aggregation with privacy is to develop new techniques to handle the privacy and anonymity while ensuring meaningful aggregation of sensor data.

XI. CONCLUSION

The demand for security in WSN became more necessary however in WSN node has some limitation of processing storage capacity and energy. Two measure methods for cryptography are used widely in which the symmetric key are shared by users to solve this problem we are used the public key cryptography. Here we show WSN protocol stack in which security attacks and it's countermeasures. Routing attack is more vulnerable than any other security attack.

REFERENCES

[1] Y. Wang, G. Attebury, B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Communications Surveys & Tutorials,vol.8, no.2, pp. 2-23, 2006

[2] Energy Efficiency of Symmetric Key CryptographicAlgorithms in Wireless Sensor Networks Xueying Zhang, Howard M. Heys, and Cheng Li Faculty of Engineering and Applied Science Memorial University of Newfoundland St. John's, NL, A1B 3X5, Canada.

[3] Security in wireless sensor network.Indo college of engineering, Mohali India.

[4] The Scheme of Public Key Infrastructure forImproving Wireless Sensor Networks Security ZhangYu

[5] An Efficient Pairwise Key Establishment Schemefor Wireless Sensor NetworksKun Mu, Qingmin CuiDepartment of Computer Science and EngineeringHenan Institute of Engineering Zhengzhou 451191, China

[6] Review on Security Issues and Attacks in Wireless Sensor Networks Volume 3, Issue 4, April 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[7] Rina Bhattacharya, "A Comparative Study of Physical Attacks on Wireless Sensor Networks", IJRET, vol. 2, issue 1, pp. 72-74, Jan 2013

[8] Sophia Kaplantzis, "Security Models for Wireless Sensor Networks" March 20, 2006

[9] Security For Wireless Sensor NetworkSaurabh SinghDepartment of Computer Science and Engineering, NIT,Jalandhar,Punjab, India, International Journal on Computer Science and Engineering (IJCSE)

[10] Chris Karlof David Wagner. In Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures