A Novel Authentication approach in Wireless sensor Network

Swapna Naik , Dr. Narendra Shekokar, Rupali Yavale

Abstract— WSN consists of large number of Sensor Nodes where each Sensor Nodes in the network are connected by a wireless channels. The node will sense the environmental data and sends to the other sensor nodes or Base Station. During the transmission of data from one node to another node, different security techniques are used. To implement security, such as confidentiality, integrity and authentication, keys are needed. Key Management is important for implementing security in a wireless Sensor Network. Wireless Sensor Networks are believed to be the enabling technology for ambient intelligence. The common attacks that can be made on WSN are attacks like eavesdropping, man-in-the middle attack and passive attacks like replay attacks, DoS attacks, and cloning attacks. An authentication protocol can enable the senders to confirm that the packet was truly sent to authentic receiver. Our solution achieves proper authentication while keeping energy consumption at minimum . A separate key for each node to node communication is generated so that detection of malicious node is easily possible.The use of timestamping provides additional security.

Keywords-Node deployment, Wireless Sensor Network, Authentication, Public Key Cryptography.

I. Introduction

The concept of wireless sensor networks is based on a simple combination of Sensing function with CPU and Radio which opens the possibility to thousands of potential applications. Securing wireless sensor networks , is particularly challenging because of the following constraints

- Limited memory resources and the inability to store data about all devices it will possibly need to authenticate with prior to deployment.
- Their ad-hoc nature, potentially forcing sensor nodes to interact with many different networks over time.
- Sensor nodes are not tamper resistant, therefore keying material, data and code can be extracted.
- With no online certificate authority to reference and no Internet connectivity the usage of a conventional PKI architecture is severely restricted.

Each individual node must be designed to provide the set of primitives necessary to produce the interconnected network that will emerge as they are deployed, at the same time meeting strict requirements of size, cost and power consumption[8].

The Wireless communication is subjected to threats such as Denial of sleep attack, Jamming attack ,Replay attack, Flooding attack ,Selective forwarding attack. Ensuring proper authentication is the only way to protect the communication against attacks. Wireless sensor nodes have to work using their limited supply of energy for performing, computations and transmitting information in a wireless environment, as the recharging or replacing of power resources might not be possible. The lifetime of a sensor network is dependent on the lifetime of a node.

Security is critical for sensor networks deployed in hostile environments, such as military battlefields and security monitoring. In typical sensor networks, a sensor node uses multi-hop wireless transmissions to communicate with a base station or other nodes. The key challenge is to keep this communication secure [8].

In symmetric key based techniques, nodes share a secret key and compute a message authentication code. The shared keys may remain unchanged for some time and make the network vulnerable to spatial and temporal replay attacks. During the authentication process, some secret information is mutually agreed upon so that the communication can proceed efficiently in protected mode to achieve desired confidentiality this can be done using modern digital and cryptographic techniques

The vital constraints in WSN are fault tolerance, scalability & production network dynamics, transmission media, coverage, connectivity, self-configuration, Quality of service which depends on the Battery life of the sensor node which can be preserved by preventing power consumption attacks by implementing Security. The security mechanism must also be lightweight enough so that the overhead from encryption does not affect the QoS of the network.

This paper is organized as follows: section 2 discusses the various type of attacks which pose a threat to security of wireless sensor nodes. Section 3 presents existing authentication techniques which are presently being used in wired environment as well as in wireless architectures also. Literature survey of the various authentication and data encryption techniques is carried out in section 4. Section 5 consists of the conclusion followed by the reference listing.

II. SECURITY ATTACKS

In the following section we discuss the various threats and attacks on WSN and the damage which each of them does to WSN.

A. Data integrity and confidentiality related

These types of attack attempt to reveal or compromise the integrity and confidentiality of the data contained in the transmitted packets. Some attacks are Denial of Service on Sensing (DoSS) attack the attacker tampers with data before it is read by sensor nodes, therefore resulting in false reading. Targeting the physical reading.In the Node Capture attack attacker physically captures sensor nodes and compromises them such that sensor readings are inaccurate and manipulated , whereas in eavesdropping attack the attacker eavesdrops on ongoing communications between targeted nodes to collect information on connection & cryptography.

B. Power consumption attacks

These types of attack attempts to exhaust the device's power supply. Worst case would collapse a network communication. Some of the attacks are Denial of Sleep attack where the attacker tries to drain a wireless device's limited power supply so that the node's lifetime is significantly shortened. Normally MAC reduces power consumption by regulating the node's radio communication. The attacker attacks the MAC layer protocol to shorten the sleep period, or disable the sleep period.

C. Service availability and bandwidth consumption attacks

They also can be categorized as power consumption related attacks. They mainly aim to overwhelm the forwarding capability of forwarding nodes, or consume sparsely available bandwidth. Some known attacks are Flooding Attack, Jamming Attack, Replay Attack and the Selective Forwarding Attack.

D. Routing attacks

These attacks attempt to change routing information, and to manipulate and benefit from such a change .Some known attacks are: Unauthorized routing update attack, Wormhole Attack, Sinkhole attack. These types uncover the anonymity and privacy of the communications and in the worst case scenario, can cause false accusations of an innocent victim . One of the known attack is the Traffic Analysis Attack where attacker attempts to gain knowledge of network, traffic and nodes behaviour.

III. AUTHENTICATION MECHANISMS

Security by authentication in sensor networks is dependent on what we are trying to protect. There are four security goals in sensor networks which are Confidentiality, Integrity, Authentication and Availability. Confidentiality is the ability to conceal message from a passive attacker, where the message communicated on sensor networks remain confidential. Integrity refers to the ability to confirm the message has not been tampered, altered or changed while it was on the network. Authentication is the confirmation or assurance that the messages are from the node it claims to be from, thus determining the reliability of message's origin. Availability is to determine if a node has the ability to use the resources and the network is available for the messages to move on. Freshness implies that receiver receives the recent and fresh data and ensures that no adversary can replay the old data. This requirement is especially important when the WSN nodes use shared-keys for message communication, where a potential adversary can launch a replay attack using the old key as the new key is being refreshed and propagated to all the nodes in the WSN. This can launch attacks such as disrupting or disabling the network by overloading it with messages.

When authentication is based on public key any of the encryption algorithms using public key can be used to encrypt the data the Public-key cryptography, also known as asymmetric cryptography, refers to a cryptographic algorithm which requires two separate keys one of which is private and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt cipher text or to create a digital signature. The term "asymmetric" arises from the use of different keys to perform these opposite functions, each the inverse of the other as opposed to conventional ("symmetric") cryptography which relies on the same key to perform both.

Public-key algorithms are, mainly based on mathematical problems which are difficult to solve, mostly involving certain integer factorization, discrete logarithm, and elliptic curve relationships. It is computationally easy for a user to generate his or her public and private key-pair and to use them for encryption and decryption. The strength lies in the fact that it is computationally very difficult or impossible for a properly generated private key to be determined from its corresponding public key.

Message authentication involves processing a message with a private key to produce a digital signature. Thereafter anyone can verify this signature by processing the signature value with the signer's corresponding public key and comparing that result with the message, if it matches then authentication is Successful [8].

Public-key algorithms are fundamental ingredients in security applications and protocols. Some public key

algorithms provide key distribution and secrecy e.g. Diffie–Hellman key exchange, some provide digital signatures e.g. Digital Signature Algorithm, and some provide both e.g. RSA [10].

Diffie-Hellman key exchange uses the integers between 1 and p−1 where p is a prime are used with normal multiplication, exponentiation and division, except that after each operation the result keeps only the remainder after dividing by p. The two parties Alice and Bob need to choose two numbers p and g; where p (modulo) is a prime number and the second number g is a primitive root of order (p-1) in the group 1 to p-1 and is called the generator. The two numbers are public and can be sent through the Internet [4].

Elliptic curve cryptography [ECC] is a public-key cryptosystem just like RSA, Rabin, and El Gamal. An elliptic curve is a plane curve defined by an equation of the form y2=x3+ax+b. A two variable equation F(x, y)=0, forms a curve in the plane. We are seeking geometric arithmetic methods to find solutions. Elliptic curves are used as an extension to other current cryptosystems like Elliptic Curve Diffie-Hellman Key exchange, Elliptic Curve Digital Signature algorithm. In this both parties agree to some publicly-known data items like the elliptic curve equation , the values of a and b, prime p. The elliptic group computed from the elliptic curve equation. A base point B, taken from the elliptic group Similar to the generator used in current crypto systems. Each user generates their public/private key pair where Private Key is an integer, x, selected from the interval [1, p-1] and the Public Key = product, Q, of private key and base point (Q = x*B) [5].

Elliptic curve cryptography is much faster and requires less memory therefore it is suitable for wireless sensors . So we can even carry out the Diffie-Hellman key exchange using the Elliptic curve cryptography.

IV. RELATED WORK

The main purpose of node authentication is to effectively shield the sensor nodes against attack by a malicious node. Manish P. [2] proposes a network structure consisting of base station, cluster head and member nodes. Before the actual deployment takes place for each of the nodes in the network, a unique fingerprint for each sensor node is generated. This is done by combining relative nodes information through a superimposed s-disjunct code. This is unique fingerprint is loaded into each node Post-deployment phase public key N generation by the base station is done. Basically this key is used by any two nodes at a given time while communicating.. By using Zero Knowledge Protocol for k times per communications verifier will continue the authentication process which includes number of verification rounds.

A Jayanthiladevi et al [3] has further improved on the above by suggesting that secured communication can be realized using user authentication concept but also points out that public key cryptography is used when there is large number of user due to its scalability. Here sensor communicates among each other with the help of symmetric cryptography. The user and timestamp's validity is verified by the gateway node. The focus is on the cluster based key management technique for optimizing overhead and providing authentication in wireless sensor networks.

Mahmood Khalel et al [4] points out Diffie-Hellman algorithm are vulnerable to the man-in-the-middle attack in which the attacker is able to read and modify all messages between Alice and Bob., The man-in-the-middle attack can be prevented by a station-to-station key agreement by using digital signature with public key certificates to establish a session key between Alice and Bob.

A modified version using zero knowledge with Diffie-Hellman is suggested where a trusted third party selects two prime numbers p and g, and announces them as public numbers.

Samant et al [5] have presented modified version of Diffie- Hellman. It is implemented using Elliptic Curve Cryptography (ECC) over GF (2m) in order to obtain stronger cryptography. In this paper using Koblitz curves and TNAF (τ - adic non-adjacent form) with partial reduction modulo. A Diffie-Hellman key exchange is implemented. The advantage of using Partial Reduction Modulo is to reduce the length of the TNAF without making the security level less which reduced the calculation time by 34.5%.

L.B. jivandham et al [6] proposed security protocol which integrates one round Zero Knowledge Proof and AES algorithm for node authentication, where only authenticated nodes will be accepted during node-move-in operation. The proposed system shows that it requires O(h+q) rounds for a node to join into a network securely, where h is the height of the dynamic cluster-based wireless sensor network and q is the number of neighboring nodes of a joining node. Based on the protocol, both base station and new node know generator g, b and prime number p. It is a challenge-and-response kind of protocol where new node has to prove its authenticity using zero knowledge. The network key is generated by the base station using the AES algorithm. This is the symmetric key that allows new node to join the network and for all nodes .

V. PROPOSED SYSTEM

In our proposed architecture there are three layers in the network, where Base Station constitutes the first layer. The Base Station controls the cluster heads and all the nodes in the cluster which constitute the second layer and the third layer respectively.

Clusters are made of a cluster head under it there are a number of sensor nodes. The communication can take place between Base Station and cluster nodes as well as the sensor nodes. The cluster nodes have direct

communication with any sensor node under a cluster, at the same time it can communicate with other cluster nodes or with the Base Station.

The base station is typically a gateway to another network, a powerful data processing or storage center, or an access point for human interface. They can be used as a nexus to disseminate control information into the network or extract data from it.

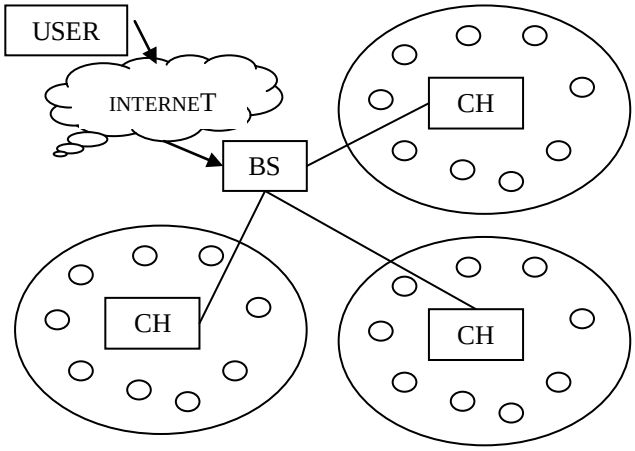

Fig 1 : clusters and base station

previous work on sensor network routing protocols, base stations have also been referred to as sinks. Base Stations are typically many orders of magnitude more powerful than sensor nodes. They might have workstation or laptop-class processors, memory, and storage, AC power, and high-bandwidth links for communication amongst themselves. So there is a distinct difference of capability between sensor nodes and their base station. In our proposed system network of sensor nodes forms a multi hop wireless network to allow sensors to communicate to the nearest base station.

A Key Distribution Server (KDS) provides Node with a special key & unique id before deployment. We first identify all the secure nodes initially and syn chronize their clocks to a common value.

A. Key Derivation

Each node computes its original key using the pseudorandom function, special key and unique id. This random function takes into consideration the special key and the unique id to compute the original key called K. Mutual authentication check is carried out using k between Base station and cluster nodes and then cluster and sensor nodes.

When we are carrying out the authentication between cluster head to sensor, the Cluster node computes Bij=H (Idi||T) where i is the cluster node, j is the sensor node to be authenticated, T1 is the current timestamp of cluster node i. IDi and is the unique id of cluster node i. node i sends a message (Bij,T) to sensor node j. The sensor node j checks for the validity of the timestamp.

B. Timestamp Validation

For time stamping we are using the following condition. If at time T1, A sends a synchronization pulse packet to B. Node B receives this packet at T2, where T2 =T1+d+δ. Here, δ and d represent the offset between the two nodes and end-to-end delay respectively. At time T3, B sends back an acknowledgement packet. This packet contains the values of T2 and T3. Node A receives the packet at T4.

So (T'-T) <=ΔT, T' is the current timestamp of sensor node and ΔT is the time interval of transmission between I and j. If this condition not satisfied then it means that sensor node j has failed the authentication check and cluster node i gets to know that j is a malicious sensor node and breaks down the communication with sensor j.

If the condition is satisfied then sensor node j computes: Bji=H(IDi || T) where T is the current timestamp of sensor j. Now sensor j compares the value of Bji with the received value of Bij. If they are equal then cluster node i knows that sensor j has been authenticated successfully.

For authentication between Base Station to cluster head secondary key is used. This is a unique value for each cluster head to Base Station communication. It is calculated as is Ks→ci =H(k||Idi). Where Idi is the id of the cluster node, K is the original key and H is the hash function. The S denotes Base station and a particular cluster is ci. Here IDi is the id of the cluster node, K is the original key and H is the hash function. This secondary key enables the server to choose the cluster nodes.

When authenticating the communication between Base station and sensor node. The Base station establishes another key for direct communication with the sensor nodes and it is called the tertiary key. It is calculated as Kci→sj=H(K||Idi) in this Ci= cluster node, sj= sensor node.

To enhance security further we can use elliptical curve cryptography using Diffie exchange to authenticate the Base station to the cluster heads. Since symmetric keys can become compromised after some period . A malicious node may get access to all node information by pretending to be the Base station in which can cause a serious security lapse . Since the Base station is generally laptop class, we can use the low power consuming elliptic curve cryptography to authenticate the base station.

Table 1: Comparison of key sizes

Security level (in bits)	*Symmetric scheme (key size in bits)*	*ECC-based scheme (size of n in bits)*	*DSA/RSA (modulus DSA/RSA (modulus size in bits)*
56	*56*	*112*	*512*
80	*80*	*160*	*1024*
112	*112*	*224*	*2048*
128	*128*	*256*	*3072*

Table 1 shows an analysis of the key sizes required for various type of cryptography ,this shows that we can use symmetric keys at node levels since node energy is limited . The base station authentication using elliptical curve cryptography is also energy saving compared to other public key methods.

The sensors in the communication range serve as promoters between public key cryptography of the user and symmetric crypto world of WSN. The user communicates to sensors with the help of public key cryptography and sensors communicate to the rest of the sensor network using symmetric cryptography. Symmetric key size is least as compared to elliptic curve cryptography which still requires less key size when compared to DSA and RSA. The computation overhead of symmetric key is much less as compared to ECC based scheme , so we can always use it along with hashing to carry out symmetric encryption at the node level.

VI. CONCLUSION

In this paper we have proposed a technique which uses hierarchy in nodes to generate unique identification for each node. Our system presents a unique Key generation and distribution mechanism, whose main objective is to provide reliable and secured communication, which is the most fundamental security service in WSN. By using different authentication mechanism for each hierarchy of the node in the cluster we can limit the damage which may be caused by the introduction of malicious node. Communication between base station and the internet can be carried out using public key cryptography. Sensor nodes have limited capabilities and resources. More importantly excessive use of resources may result in a decrease in network lifetime. Securing the communication of location information also requires extensive processing and special communication protocols to ensure the information authenticity. Managing power consumption efficiently while communicating securely within the network is an important issue. A novel security framework that provides a comprehensive security solution against the vulnerabilities of WSN has been proposed. This supports the four main tenets: an authentication mechanism, a key management scheme, an encryption mechanism and a localization scheme.

REFERENCES

[1] Siba K. Udgata, Alefiah Mubeen and Samrat L. Sabat, "Wireless Sensor Network Security model using Zero Knowledge Protocol, "Proceedings of 2011 IEEE International Conference on Communications, ICC, page 1-5. IEEE 2011.

[2] Manish P. Gangawane," Implementation Of Zero Knowledge Protocol In Wireless Sensor Network for prevention Of Various Attacks," International Journal of Emerging Technology and Advanced Engineering , (ISSN 2250-2459, Volume 2, Issue 8, August 2012).

[3] A Jayanthiladevi, S Suma and T.Lalitha, "Challenges and Authentication in Wireless Sensor Networks," 2013 IEEE.

[4] Mahmood Khalel, Ibrahem and Al Nahrain," Modification of Diffie–Hellman Key Exchange Algorithm for Zero Knowledge Proof," proceedings of 2012 international conference on future c ommunication networks, IEEE 2012.

[5] Samant Khajuria and Henrik Tange, "Implementation of Diffie-Hellman Key Exchange on Wireless Sensor Using Elliptic Curve Cryptography," proceedings of IEEE 2009.

[6] L. B. Jivanadham ,A.K.M. ,M. Islam2 and Mansoor3,"A Secured Dynamic Cluster-Based Wireless Sensor Network Advanced Informatics School (AIS)," proceedings of 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks, IEEE 2012.

[7] Feng Yang and Xuehai Zhou, "Distributed Node Authentication in Wireless Sensor Networks ," [Volume 1] 2010 2nd International Conference on Future Computer and Communication V1-73.

[8]Jason Lester Hill ," System Architecture for Wireless Sensor Networks," a project report for B.S. (University of California, Berkeley998 M.S.

[9] K.S.Arikumar, K.Thirumoorthy, " Improved User Authentication in Wireless Sensor Networks," proceedings of ICETECT 2011, 2011 IEEE.

[10]Mircea Frunza and Luminita Scripcariu, "Improved RSA Encryption Algorithm for Increased Security of Wireless Networks," IEEE 2007.