IJMTST | Volume: 2 | Issue: 05 | May 2016 | ISSN: 2455-3778

# Securing the Data Communication between the Neighboring Sensor Nodes using Bilinear Pairing for Source Location Privacy in Wireless Sensor Network

Mr. Mohammed Azharuddin[1] | Mrs. Veena M[2]

[1]M.Tech Scholar, Department of CS&E, P.E.S College of Engineering, Mandya, Karnataka, India
[2]Asst. Professor, Department of CS&E, P.E.S College of Engineering, Mandya, Karnataka, India

## ABSTRACT

*Privacy of data is one of the most important concept in wireless sensor networks. Wireless sensor networks are used in many areas likewise in tracking and monitoring of some events. Each sensor node has one private key and an assigned id. We are providing data confidentiality between the sensor nodes in wireless sensor network using bilinear pairing (diffie-hellman algorithm). Sharing of data between those neighbouring nodes is also secured with the concept of shared secret key(symmetric key cryptography). Content privacy and context privacy can be obtained and the threats regarding to it can be overcomed. Data is encrypted between the nodes using those shared secret keys. We are providing security for the data between the neighbouring nodes in wireless sensor networks.*

**KEYWORDS:** *Wireless sensor nodes privacy, privacy preservation of data, content privacy and context privacy, bilinear pairing, shared secret key*



## I. INTRODUCTION

Wireless sensor network are spatially distributed, autonomous sensors to monitor physical or environmental conditions and to co-operatively pass their data through the network to a main location. The development of wireless sensor networks is motivated by military applications such as military surveillance application and tracking animal activity etc. Wireless sensor network is built of nodes from a few to several hundreds or even thousands. Each sensor node has typical parts such as a radio transceiver with an internal antenna. WSN nodes can be categorized as source node, sink node and intermediate nodes depending upon functionality in environment.Source node is the node to transmission of some kind of information as reaction to some event occurring in its sensing range. Intermediate node is used as data forwarders in multi hop communication [1]. Sink node is control all over that node present in sensing range and Sink gathers the sensed data from the entire nearby node for final processing.

It is providing source node privacy by maintaining data confidentiality between the neighbouring nodes with the help of the shared secret key. Each sensor node has one private key and an assigned id. Sensor nodes with the help of the private keys and assigned id's can create a shared secret key between them through which data is shared securely. So that the neighbouring nodes encrypts the data using shared secret key. Sensor network is categorised into content privacy threats and context privacy threats.

Content privacy threats generate due to the ability of adversary to attack and observe the exact content of packet. Context privacy can be used for finding the location of the source node. The confidentiality of message is another privacy category called content privacy. Content privacy gives importance on providing integrity, non-repudiation and confidentiality of message exchange in sensor network. Context privacy comprises for instance, hiding the identity and location of each node.

## II. IMPACT OF ATTACKS IN SOURCE LOCATION PRIVACY BETWEEN THE NEIGHBOURING SENSOR NODES

We are categorizing the attacks occurring in wireless sensor network to provide data confidentiality between the sensor nodes. The attacks are as follows:

*A. Adversary attack*

Adversary can drop number of packets in simulation time. It can insert its own packets into the network. Internal adversary can compromise a node within the sensor area. Whereas an external adversary cannot do that.Internal adversary has access to components and an external adversary does not have permission to access. The active attacks of the adversary comprise injecting false packet into the dropping actual packet network traffic. Passive attack is eavesdropping in which adversary listens to the traffic and tries to capture the content that is exchanged between the node [2, 4].

*B. Eavesdropping attack*

The Eavesdropping attack is a serious security threat to a sensor network. Conventional sensor area consist of wireless nodes equipped with Omni-directional antennas, which broadcast radio signals in all directions and are consequently prone to the eavesdropping attacks. For Passive Eavesdropping in which the malicious nodes detect the information by listening to the message transmission in the broadcasting wireless medium. For Active eavesdropping where the malicious nodes actively grab the information via sending queries to transmitters by disguising themselves as friendly nodes. For eavesdropping attacks they are using cluster based anonymization techniques to protect from those attacks [2, 11].

*C. Compromised node*

Adversary uses a compromised node to influence the protocol or to detect other node. Adversary can also destroy a node in this case. Adversary uses a compromised node to get information such as the identity of a node, the information received and sent by node and encrypt keys of a node. Compromised node can send packet to real node to access data in unauthorized way. On that node they can access data from different node. Fake node used for to confuse compromised node packet attack in sensor area [1, 2].

## III. EXISTING SCHEME

In this paper we discuss the earlier schemes that are described to provide source location privacy and privacy between the sensor nodes.

*A. Adversary attacks*

In next techniques [1, 13], anonymous concept is used to hide real identity from adversary node attacks. To preserve source location privacy becomes important in wireless sensornetwork. The privacy threat occurring for sensor networks may be divided in different categories that iscontent privacy and context privacy. Those techniques are used to hide sensitive information in source location privacy. They propose a source location privacy scheme for WSN through cluster based anonymisation. It must hide real identity during communication.

*B. One way hash chain*

Kantha Kumar Pongaliur et al [2] also introduced a sensor network that uses either selecting random path to make it hard for an adversary to track real identity. They mention that hiding source information using cryptographic techniques incurring lower overhead. The adversary model considers a super local eavesdropper having the ability to compromise sensor node. They are provided source privacy under eavesdropping and node compromise attacks. They use a one way hash chain based keying mechanism to hide the source information.

*C. Safety period*

Mauro conti et al [3], they provide a survey of state in source location privacy. It mentions key concepts in source location privacy, such as anonymity, unobservability, and safety period.

*D. Information leakage*

In this paper [4], they proposed a solution for the source location privacy from information leakage problem. They proposed it to quantitatively measure source location information leakage in routing based source location privacy. It identifies vulnerabilities of some well-known source location privacy protected schemes. It is mentioned to provide source location privacy through routing to a randomly selected intermediate node and network mixing ring. The aim is to provide excellent source privacy under adversary attacks.

*Disadvantages of the existing scheme*

The disadvantages of all these existing schemes provided in wireless sensor network can be listed as follows:

- It is not providing guaranteed performance in energy consumption.
- The performance is low when related to the terms of memory consumption.
- It is not providing guaranteed performance for message delivery latency.
- There is no secured data confidentiality between the neighbouring sensor nodes.

## ENHANCED SHEME FOR PRIVACY OF NEIGHBOURING NODE UNDER ATTACKS

*A. Source privacy under attacks*

Our aim is to maintain source privacy under compromise node, eavesdropping, misbehaving node. Misbehaving node is tried to send packet at real node and capture information from that node.

Main objective of source privacy under attacks is as follows:

- To measure energy consumption.
- To improve accuracy, data confidentiality in secure WSN.
- To impact network density using fake node and fake packet.
- To check the performances under attacks and evaluate performance metrics.
- To achieve high message delivery ratio, packet drop ratio.

*B. Communication of data between neighbouring nodes using bilinear pairing(Diffie-Hellman algorithm)*

Each sensor has one private key and an assigned id. We are generating shared secret key between the neighbouring sensor nodes by taking the private keys and assigned id's of those nodes, with the help of private keys and assigned id's of those sensor nodes a shared secret key is generated between them through which they can encrypt the data. If the neighbouring nodes do not have the shared secret key, data sharing is not possible between them. Shared secret key is used for securing the communication with the neighbour node.

To generate a shared secret key, we are using bilinear pairing concept that is Diffie-Hellman algorithm. The algorithm is as follows:

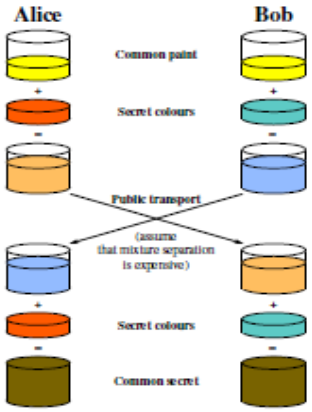


Fig: Illustration of Diffie-hellman key exchange

Diffie–Hellman algorithm establishes a shared secret key that can be used for secret communications while exchanging data over a public network. The following diagram illustrates the general idea of the key exchange by using colours instead of a very large number. The crucial part of the process is that Alice and Bob exchange their secret colours in a mix only. Finally this generates an identical key that is computationally difficult (impossible for modern supercomputersto do in a reasonable amount of time) to reverse for another party that might have been listening in on them. Alice and Bob now use this common secret to encrypt and decrypt their sent and received data. It should be noted that the starting colour (yellow) is arbitrary, but is agreed on in advance by Alice and Bob. The starting colour is assumed to be known to any eavesdropping opponent. It may even be public.

*Cryptographic explanation with an example*

The simplest and the original implementation of the protocol uses the multiplicative group of integers modulo*p*, where *p* is prime, and a primitive rootmodulo*p*. Here is an example of the protocol, with non-secret values in blue, and secret values in red.

1. Alice and Bobagree to use a prime number p= 23 and base g =5 (which is a primitive root modulo 23).
2. Alice chooses a secret integer a=6, then sends Bob A = $g^a \bmod p$
   - A = $5^6 \bmod 23 = 8$

3. Bob chooses a secret integer b = 15, then sends Alice B = $g^b \bmod p$
   - B = $5^{15} \bmod 23 = 19$
4. Alice computes s = $B^a \bmod p$
   - *s = $19^6$ mod 23= 2*
5. Bob computes s = $A^b \bmod p$
   - *s = $8^{15}$ mod 23 = 2*
6. Alice and Bob now share a secret (the number 2).

*Symmetric key cryptography*

The data to be exchanged between the neighbouring nodes gets encrypted using shared secret key(symmetric key cryptography). Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing.

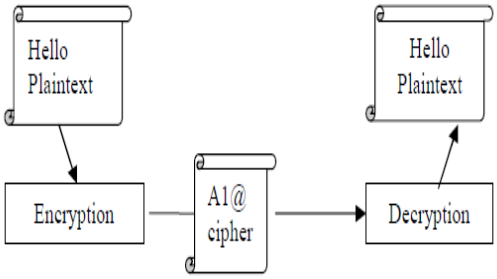


Fig: Secret key cryptography

A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plain text block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plain text will encrypt to different cipher text in a stream cipher. Self synchronizing stream ciphers calculate each bit in the key stream as a function of the previous n bits in the key stream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit key stream it is. Synchronous stream ciphers generate the key stream in a fashion independent of the message stream but by using the same key stream generation function at sender and receiver. While stream ciphers do not propagate transmission errors, they are, by their nature, periodic so that the key stream will eventually repeat.

## CONCLUSION

In this paper we have developed an enhanced algorithm to introduce security of data between the two neighbouring sensor nodes in wireless sensor networks. It can protect source privacy under eavesdropping attacks while also avoided node compromise attacks are presented. Simulation results demonstrate that proposed schema can achieve very good performance in energy consumption, memory consumption and message delivery latency, while assuring a high message delivery ratio.Hence we generate a shared secret key using bilinear pairing(Diffie-hellman algorithm). The data to be exchanged between the two neighbouring sensor nodes gets encrypted using shared secret key(Symmetric key cryptography). Hence the confidentiality of the data can be obtained in a secured way in wireless sensor networks.

## REFERENCES

[1] AparnaGurjar,A R BhagatPatil,"Cluster based Anonymization for Source location privacy in wireless sensor Network" International Conference-2013.

[2] Kantha Kumar Pongaliur and Li Xiao,"Sensor Node Source Privacy and Packet Recovery under Eavesdropping and Node Compromise Attacks ", ACM Trans-July 2013.

[3] Mauro Conti, JeroenWillemsen, and Bruno Crispo,"Providing Source Location Privacy in Wireless Sensor Networks: A Survey" IEEE Communications Survey & Tutorials, 2013.

[4] Basel Alomair, Member, Andrew Clark, Student Member, Jorge Cuellar and RadhaPoovendran"Toward a Statistical Framework for Source Anonymity in Sensor Networks", , IEEE, Transactions ,FEBRUARY 2013.

[5] Yun Li, JianRen,"Quantitative Measurement and Design of Source-Location Privacy Schemes for Wireless Sensor Networks" IEEE, 2012.

[6] Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, "A Cloud Based Scheme for Protecting Source Location Privacy against Hotspot- Locating Attack in Wireless Sensor Networks" Fellow, IEEE Transactions, October 2012.

[7] Shehla S Rana, Nitin H. Vaidya "A new „Direction" for Source Location Privacy in Wireless Sensor Networks".

[8] Wei Tan, KeXu, Senior Member, IEEE, and Dan Wang,"An anti-tracking source-location privacy protection protocol in WSNs based on path extension" IEEE,2012.

[9] Rongxing Lu, "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", IEEE, Transactions, MARCH 2013.

[10] Jian Li, Yun Li, JianRen," Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor

Networks" Senior Member, IEEE, Transactions ,MAY 2014.

[11] Wuchen XIAO, Hua ZHANG, Qiaoyan WEN, Wenmin LI, "Passive RFID-Supported Source Location Privacy Preservation against Global Eavesdroppers in WSN", IEEE IC-BNMT2013.

[12] Long1, Mianxiong Dong2, Kaortu Ota3, And Anfeng Liu1, "Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-Based Diversionary Routing in Wireless Sensor Networks" ,2014.

[13] Yun Li and JianRen "Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks" IEEE INFOCOM 2010.

[14] PandurangKamat, Yanyong Zhang, Wade Trappe, CelalOzturk "Enhancing Source-Location Privacy in Sensor Network Routing".

[15] NiteshGondwal, ChanderDiwaker "Detecting Blackhole Attack in WSN by check Agent using Multiple Base Stations"international journal 2013.

[16] IEEE Communications Magazine Homepage | IEEE Communications Society. Cosmoc.org. Retrieved on 2013-10-29.

[17] S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-hall, Inc., 1999 pp 23-50.