WWJMRD2017; 3(10): 158-161
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Gagandeep Kaur
M. Tech (Student)
Department of Computer
Science and Engineering
GZS Campus College of
Engineering & Technology,
Bathinda, India

Dinesh Kumar
Associate Professor
Department of Computer
Science and Engineering
GZS Campus College of
Engineering & Technology,
Bathinda, India

A Location-Aware Authentication for structured Network and structured Key Management Scheme for Wireless Sensor Networks

Gagandeep Kaur, Dinesh Kumar

Abstract

As Sensor Nodes are deployed randomly in an uncontrolled environment used to collect the information and they communicate with base station using the transceiver. These are selected based on the parameters like Computation Rate, Processing Speed, Storage & Communication Range required for the network. Typically, ensuring security in wireless sensor network consists in providing confidentiality, authentication, and integrity services for the exchanged data that are mainly implemented using encryption algorithms where a number of keys need to be shared between the network elements. WSN can be sometimes insecure due to the presence of the malicious node which can destroy the network traffic. But sometimes it may be possible that certain attacker node unnecessarily sniffs the data. While data transfer from the sensor node to the cluster head or through certain intermediate relay node to the base station. There may be malicious intermediate node which read the data without permission. Even alter the data. To protect the network traffic from such kind of attackers structured key is the best way. While using structured key various performance parameters has improved compare to the base technique. There is a improvement in latency, energy dissipation and network load.

Keywords: Online Social Network, Filtering technique, Expert System, User wall, keyword filtering

Introduction

Wireless Sensor Network is a configuring network consisting of large number of tiny, cheap sensor nodes also called as “Mote”. However Sensor nodes are capable of monitoring its physical or environmental conditions without the intervention of human.WSN are implemented in an uncontrolled environment where the chances of security attacks are more. It can be used to collect and report the information to control center about an event occurred using wireless transmission. As Sensor Nodes are deployed randomly in an uncontrolled environment used to collect the information and they communicate with base station using the transceiver. These are selected based on the parameters like Computation Rate, Processing Speed, Storage & Communication Range required for the network. Typically, ensuring security in wireless sensor network consists in providing confidentiality, authentication, and integrity services for the exchanged data that are mainly implemented using encryption algorithms where a number of keys need to be shared between the network elements.

Security Measures

Asymmetric Cryptography in WSNs: The asymmetric cryptography is to load secret information in the sensor nodes before their deployment in the network. This secret information may be the secret key itself or auxiliary information that helps the sensor nodes to derive the real secret key. With this secret key, nodes can securely communicate.Public key cryptography – Mathematically related key pair (public key, private key) For Example: RSA, Elliptic Curve Cryptography. ECC is a public key encryption based on elliptic curve theory that can be used to create faster, smaller & more efficient cryptography keys.

Correspondence:
Gagandeep Kaur
M. Tech (Student)
Department of Computer
Science and Engineering
GZS Campus College of
Engineering & Technology,
Bathinda, India

Literature Survey

W. Abdullah (2016) [6] et al: This paper, proposes a location aware key authentication and distribution mechanism to secure WSNs where the key establishment is performed using elliptic curve cryptography and identity-based public key scheme. In this scheme, public key authentication is based on the position of the sensor node in the monitored area. Based on the information collected by sensor nodes.

D. Huang (2014) [2] et al: Sensor networks are composed of a large number of low power sensor devices. Recently, several pair wise key schemes have been proposed for large distributed sensor networks. These schemes randomly select a set of keys from a key pool and install the keys in the memory of each sensor. After deployment, the sensors can set up keys by using the preinstalled keys. Due to lack of tamper-resistant hardware, the sensor networks are vulnerable to node capture attacks.

Y. Lee (2009) [4] et al: WSANs (Wireless Sensor and Actor Networks) are proposed to overcome the limitations of traditional sensor networks. It includes mobile and resource-efficient actors within the network and enables these actors to respond appropriately

D. Du (2012) [7] et al: In this paper, we propose a novel key management scheme called MAKM (modular arithmetic based key management). The proposed MAKM scheme is based on the congruence property of modular arithmetic. Each member sensor node only needs to store a key seed. This key seed is used to compute a unique shared key with its cluster head and a group key shared with other nodes in the same cluster. Thus, MAKM minimizes the key storage space. Furthermore, sensor nodes in the network can update their key seeds very quickly. Performance evaluation and simulation results show that the proposed MAKM scheme outperforms other key-pool-based schemes in key storage space and resilience against nodes capture. MAKM scheme can also reduce time delay and energy consumption of key establishment in large-scale WSNs.

S. Khan(2015)[1] et al: In this paper, we present an authentication and key management scheme supporting node mobility in a heterogeneous sensor networks that consists of several low capabilities sensor nodes and few high capabilities sensor nodes.

Algorithm

Step1: Set up the network for Local area with given number of wireless sensor nodes.
Step2: Localize the nodes either automatically and manually.
Step3: Each Sensor node senses the physical and environmental factor from environment.
Step4: Sensed data will be shared to the cluster head and base station.
Step5: While sharing the data amongst different node key will be shared. Those nodes having authenticated key will share the data.
Step6: Else locates the different path.
Step7: End

Flowchart

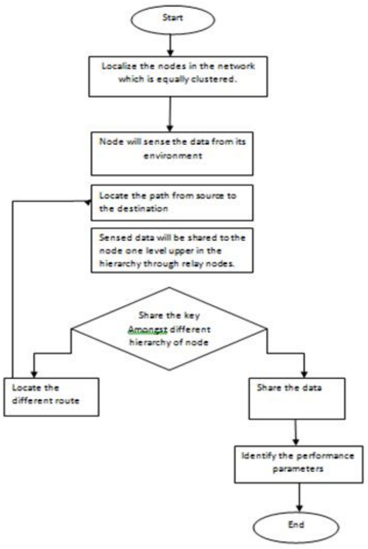

Start
Localize the nodes in the network which is equally clustered.
Node will sense the data from its environment
Locate the path from source to the destination
Sensed data will be shared to the node one level upper in the hierarchy through relay nodes.
Share the key Amongst different hierarchy of node
Locate the different route
Share the data
Identify the performance parameters
End

Fig. 1: Flow chart

Results Analysis

WSN consists of various sensor nodes distributed randomly in the specified area. Various sensor nodes location is known, such that one sensor node can always know the location of its neighbor. So that while signal transfer source node can considers the relay nodes. While data transfer between sensor node to the cluster head and then to the base station there can be any type of attacker node which can unnecessarily destroys the data packet. So for data transfer certain type of structured key management technique can be used which can protect the data from being stolen. It is one of the technique to build a secured wireless sensor network. So that network never be destroyed due to various kinds of attacks.

Parameter Taken

a. Energy Dissipation.

E_d=E_t-E_r
E_d is Energy Dissipation
I_t is Total Energy at each node
$E_r$is Energy remaining

b. Latency.

L=S_t-R_t
L is Latency.
St is the Sent Time.
R_t is Receive Time.

C. Load on each Node.

L=C-D_t
L is the Total Load at Each Node
C is the capacity of each node
$D_t$is the Total Data Transmitted

Network Configuration

Table 1: Network Configuration

Network Area	1000*1000
Number of Nodes	50
Connection Type	TCP
Application	CBR
Key	Asymmetric Key.
Antenna type	Omni directional

For building the network NS2 as network simulator is used. This network simulator has various tools to represents the all the network related configuration.

Nam File as network working

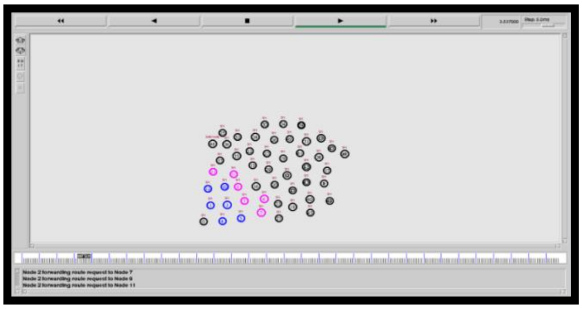

Node 2 forwarding route request to Node 7
Node 2 forwarding route request to Node 9
Node 2 forwarding route request to Node 11

Fig.2: Nam files with various network configuration

As various nodes lies in the network having randomly distributed positions. Source node identifies the path by sending the route request to the immediate neighbors. So that the path can be fixed from source to the destination through relay nodes.

Nam files for identified paths

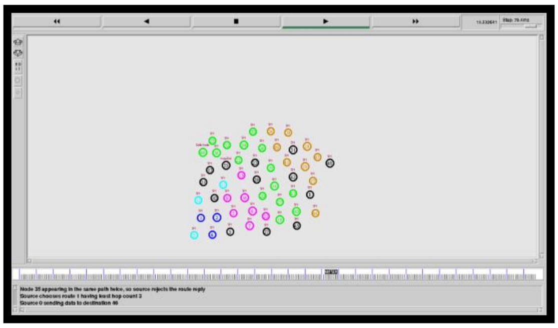

Node 35 appearing in the same path twice, so source rejects the route reply
Source chooses route 1 having least hop count 3
Source 0 sending data to destination 46

Fig.3: Figure to show the path from source to the destination

This name file shows the paths from source to the destination. There are multiple paths shown in black. One path is having minimum no. of hops while sending the data from source to the destination.

Graph for Latency

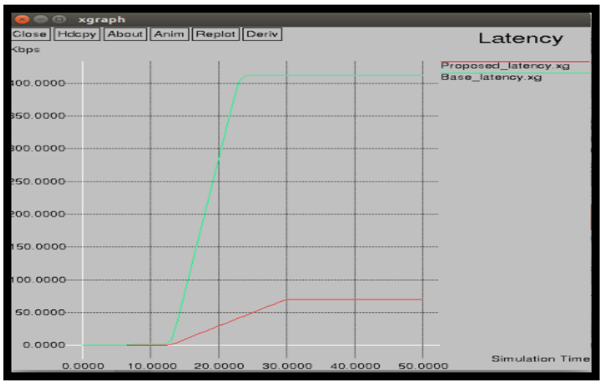


Fig.4: Graph to show the comparison of latency within old and new technique

The above figure 4 shows the comparison of latency of old and new technique. Such that proposed technique has less latency compared to the base technique. That mean less time delay is produced when certain level of security measures are being taken.

Graph for comparing the Energy Dissipation of base and New Technique

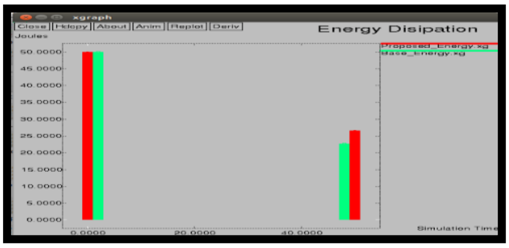
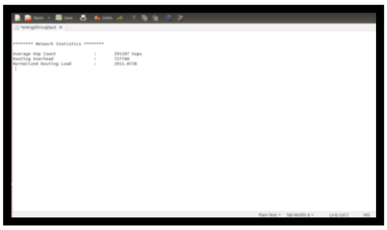


Fig. 5: Comparison graph for energy for both new and old technique

In figure 5shows the comparison of energy for both base and new technique. In case of current new research technique in which structured key system is used takes more energy compared to the base technique.

Figure to show the load on the node



```
******** Network Statistics ********

Average Hop Count               :       291107 hops
Routing Overhead                :       727760
Normalized Routing Load         :       2911.0720
```

Fig.6: figure to show the load on node

This figure shows the load on each node. This load can be routing load or it can route overhead. Such what are the extra work hashes be done by each node for successful transmission of data from source node to the destination node.

Graph for Latency

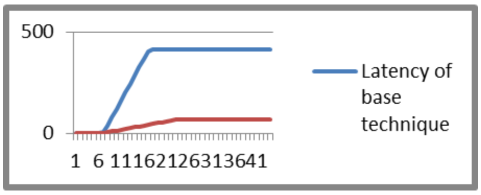


Fig. 7: figure for latency

This graph shows the latency for new technique and proposed technique. In the new technique the latency is substantially less than the base technique.

Energy dissipation graph

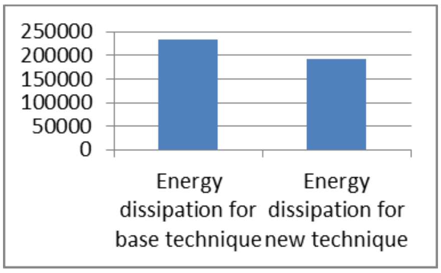


Fig 8: Energy dissipation graph.

This graph shows the energy dissipation graph for both base technique and proposed technique. In case of proposed technique the energy dissipation is little less compared to the base technique.

Load on the network

Load On the network in base technique	**Load on the node in new technique**
3010.22	2911.076

Table 2: load on the network

This table shows the network load for both base technique and the proposed technique.

Graph for load on the network

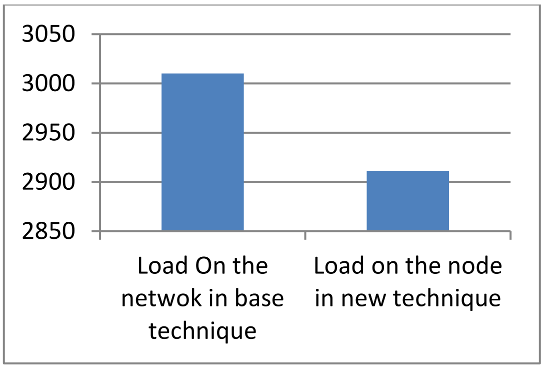


Fig. 9: Load on the network

In this figure there is a graph for network load on both base and the proposed technique.

Percentage Improvement

Parameters	Existing	Proposed	Improvement
Energy Dissipation	234302.5138	193119.1	21%
Latency	303.79	173.23	55%
Load on the network	3010.22	2911.076	3%

Table 3: of Percentage Improvement

Overall there is improvement of various parameters like energy dissipation has improved by 21%. Latency has improved by 55%. And load on the network has improved by 3%. In nutshell it is said that the results has improved compared to base technique.

Conclusion

WSN can be sometimes insecure due to the presence of the malicious node which can destroy the network traffic. But sometimes it may be possible that certain attacker node unnecessarily sniffs the data. While data transfer from the sensor node to the cluster head or through certain intermediate relay node to the base station. There may be malicious intermediate node which read the data without permission. Even alter the data. To protect the network traffic from such kind of attackers structured key is the best way. While using structured key various performance parameters has improved compare to the base technique. There is an improvement in latency, energy dissipation and network load. In future further study can be undertaken for improving the structured key so that energy dissipation can be improved further.

References

1. Khan, S., Khan, R., Bari, I., & Jan, "An Authentication and Key Management Scheme for Heterogeneous Sensor Networks",Vole. 3,pp.234-240,2015
2. Dijiang Huang, Manish Mehta, Deep Medhi, LeinHarn,"Location aware Key Management Scheme for Wireless Sensor Networks",vol. 4,pp. 29-42, 2004.
3. Ali Bagherinia, Akbar Bemana, SohrabHojjatkhah, Ali Jouharpour,"A key management approach for wireless sensor networks", Vol. 2, pp-234-240, 2014.
4. Yunho Lee, SoojinLee,"A New Efficient Key Management Protocol for Wireless Sensor and Actor Networks", Vol. 6, pp: 321-330, 2009.
5. Yu Xiuwu,FanFeisheng Zhou Lixing, and Zhang Feng,"WSN Monitoring Area Partition Clustering Routing Algorithm for Energy-Balanced", 978-1-5090-1997-7/16
6. WalidAbdallah and NoureddineBoudriga,"A Location-Aware Authentication and Key Management Scheme for Wireless Sensor Networks", vol. 3, pp: 890-900, 2014.
7. Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks", vol. 30, pp. 2314–2341, 2007.
8. F.Anjum, "Location dependent key management in sensor networks without using deployment knowledge", vol. 16, pp. 1587–1600, 2010.
9. I.-T. Kim, Y.-Y. Zhang and M.-S. Park, "An efficient location-dependent key management scheme for wireless sensor networks", in Proceedings of the Sixth International Conference on intelligent Sensors,vol. 3,pp. 245–250,2010.
10. D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography", vol. 4, pp. 71–80, 2010
11. W. Abdallah, N. Boudriga, D. Kim, and S. An, "An efficient and scalable key management mechanism for wireless sensor networks", vol. 3, pp. 480–493, 2014.
12. N. Boudriga, "On a controlled random deployment wsn-based monitoring system allowing fault detection and replacement", vol. 2014, pp. 1–12, 2014