WWJMRD 2017; 3(11): 332-336
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Renu Garg
M. Tech (Student)/PG Scholar
Department of Computer Science, Engineering
GZS Campus College of Engineering, Technology, Bathinda, India

Paramjeet Singh
Professor, Department of Computer Science, Engineering
GZS Campus College of Engineering, Technology, Bathinda, India

Correspondence:
Renu Garg
M. Tech (Student)/PG Scholar
Department of Computer Science, Engineering
GZS Campus College of Engineering, Technology, Bathinda, India

Distance adaptive routing algorithm for secured wireless sensor network while using Asymmetric Key

Renu Garg, Paramjeet Singh

Abstract
WSN is the wireless sensor network. It keeps various sensor nodes and sinks nodes. These sensor and sink nodes can be moving or stationary. On each occasion the sensor node senses the data from its environment and send that data to the sink node. If this sink node is part of IOT (internet of things) will transmit it further for further processing. While building or existence of the network any malicious node can be part of the network can destroy the network or even read the data, which is not specified to do so. Security is required for stopping these whole malicious procedures which can be the part of the network. RSA based Asymmetric key is used for providing the security. So that any sensor node while sensing the data encrypt the data with its primary key. Then at the cluster head and sink node level this data will be decrypted with private key. So that no malicious node can read the data or even understands the data. In this research providing the security has improved various parameters like packet delivery ratio, throughput, lifetime and dead node count.

Keywords: WSN, Symmetric, Asymmetric

Introduction
WSN is the wireless sensor network is consisting of various moving or stationary sensor nodes and sink nodes. This WSN is used for various applications like urban areas, Healthcare, Military surveillance etc. The sensor node needs to transfer the data to the sink node. This data can be sensitive data or it may be non-sensitive data. If it is sensitive data then it need security from intermediate relay nodes. So that no other than the actual receiver can understand the data. Each sensor node before sending the data will encrypt the data. At receiver side the data will be decrypted. Encryption at the sending end and decryption at the receiver end can be done using two types of keys. One is symmetric key, second of asymmetric key. In symmetric key same key is used for encryption and decryption. But in asymmetric key decryption key is calculated which may be different from the encryption key. Asymmetric key is more secured as compared to symmetric key.

Network Characteristics
There are various network features which make it to be used for various types of applications.
Dense sensor node deployment: Sensor nodes are densely deployed network. Various nodes are deployed close to each other. They are more densely deployed than the MANET.
Battery-powered sensor nodes: Sensor nodes main source of power is battery. There are deployed in harsh environment. So their efficient energy utilization is must.
Severe energy, computation, and storage constraints: As sensor node is having very limited energy, memory and processing resources.
Self-configurable: Sensor nodes are randomly distributed. They will configure themselves after deployment.
Unreliable sensor nodes: Sensor nodes are highly prone to various kinds of destructions. These destructions are of physical in nature due to deployment in harsh environment.
Data redundancy: The sensor nodes are set in certain environment. They will be configure and used for sensing various types of information. Because they are densely deployed there

are high chances of data correlation and redundancy.
Application specific: Sensor nodes are deployed for specific application. Design requirement can be changed if the application gets changed.
Many-to-one traffic pattern: In most sensor network applications, the data sensed by sensor nodes flow from multiple source sensor nodes to a particular sink, exhibiting a many-to-one traffic pattern.
Frequent topology change: Network topology changes frequently due to the node failures, damage, addition, energy depletion, or channel fading.

Literature Review

[1] Selva Reegan A (0216) et al: This paper has proposed a technique called as key distribution to maintain the security. WSN generally need to have secured communication for having secured application. Due to high resilience to the attacks, the pair-wise key distribution schemes are highly preferred than other schemes. However, due to the resource constraints on the nodes and the threat of node capture, pair-wise key establishment in the sensor networks is a challenging task.

[2] Ze Wang (2012) et al: To ensure secure multi-hop communication in WMN, the intra and inter domain authentication and key agreement protocols are devised sophisticatedly to achieve perfect forward secrecy and attack-resilience. It is of point of view that no other than the real user can sense the data. It always is based on mutual understanding between source and destination. So that two or more users can intercommunicates to each other for secured communication mechanism.

[3] Omar Cheikhrouhou(2015) et al: Wireless sensor Networks (WSN)consist of a large number of sensor nodes are exposed to a wide range of attacks, sensor-based applications have then to be secured. In this paper, updated survey of different Secure Group communication (SGC) schemes in WSN is used.

[4] Shio Kumar Singh (2010) et al: This paper has done a survey of routing protocols for Wireless Sensor Network and compare their strengths and limitations. Hieratical based protocols are more energy efficient. These protocols will sub divide the total network into various sub segments. Each sub segment has its own cluster head. Cluster head collects the data from its related sensor nodes and send that data to the base station.

[5] Anjali (2015) et al: Wireless sensors are small devices that have the functions of sensing, communicating, and information processing. The critical issue among Wireless Sensor Networks is energy efficient utilization of sensor nodes in order to enhance the network survivability. This paper proposes a protocol i.e. (Distance Adaptive Threshold Sensitive Energy Efficient Sensor Network) DAPTEEN based on Threshold-Sensitive Energy Efficient Sensor Network Protocol (TEEN) and Adaptive Periodic TEEN (APTEEN) hierarchical protocols for removing data redundancy and hence to enhance energy efficiency.

Algorithm

Step1 setup the network with various sensor nodes. These sensor nodes works in three hierarchy like sensor node, cluster head, base station or sink node.

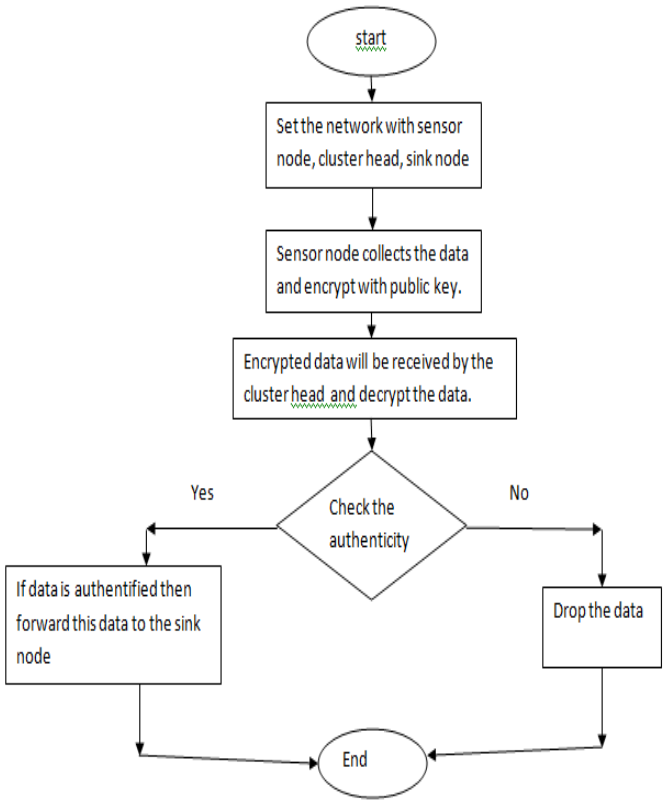
Step2 Sensor node collects the data from its environment for which it is set for.

Step3 Encrypt the data to be sent to the cluster head with the public key of the sensor node provided.

Step4 Decrypt the data at the cluster node level, checks the authenticity of the data and again encrypt the data and send to the sink node. Again it will be decrypted at the sink node level.

Step5 checks for various parameters like packet delivery ratio, Throughput, life time, dead node count.

Flowchart



Performance Parameters

Lifetime of the node in the network: It is the time for which node survive in the network communication. If the existing network node energy as resource is utilized in efficient manner. As remaining energy is directly proportional to the life time of the node.

Dead Node count: It is the nodes that loose there energy while communication. They lose the energy while relaying or transmitting the data from one node to other, finally to the base station. Their energy status becomes zero. Furthermore these nodes cannot participate in the communication.

Throughput: It is amount of data that has been either relayed or sending per unit interval of time. It shows how well node has utilized the energy for data transmitting.

Packet Delivery ratio: it is the ration of packet sent and packet received. Few packets may be lost because of security reasons or due to the lost energy at node.

Results Analysis

Network Shape

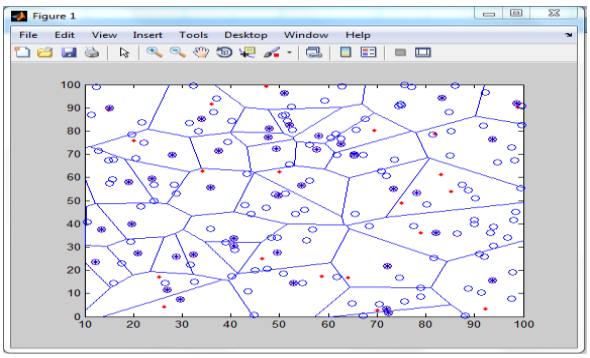


Fig. 1: Network Configuration

This figure shows the network configuration for various types of nodes like sensor node, cluster head, base station, and dead node. Each polygon shows the cluster. Each cluster includes various sensor nodes and these sensor nodes sends the data to the cluster head and then to the base station.

Lifetime of the node

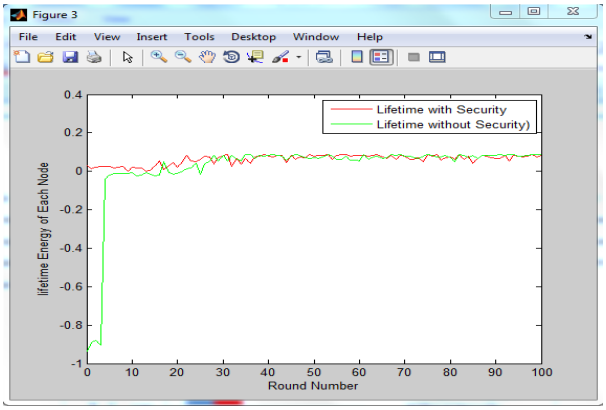


Fig. 2: Life Time comparison

This figure shows the Network Lifetime of the node in both the situation. These situations are with security and without security. Figure shows the lifetime with security has improved over to the network life time without security. As small bit of extra data also has to be transferred for maintaining the security. In the initial each node will allocated with one energy level.

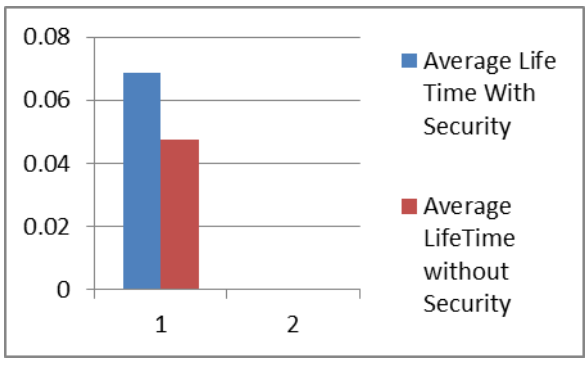


Fig. 3: Comparison of Average Life time

This graph shows that the average life time for each node has increased while the key is used in the network. Because fewer amounts of attacks will be occurred and also false reception and sending of the data will be stopped.

Throughput

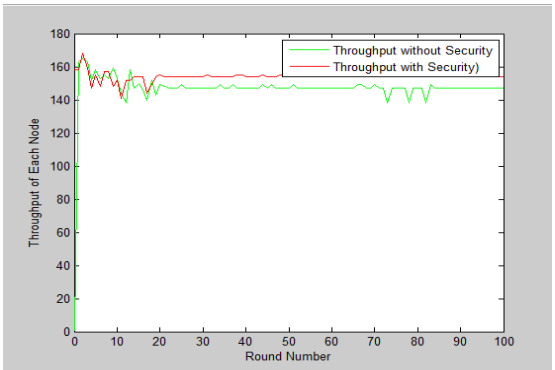


Fig. 4: Throughput comparison

This figure shows the throughput comparison for both the situations. Like throughput with security and throughput without security. Figure shows the throughput has improved in case of security. As small bit of key exchange data is also taken place in the network communication for maintaining the security. While in without security no extra bit has been transferred between source sensor nodes to the base station.

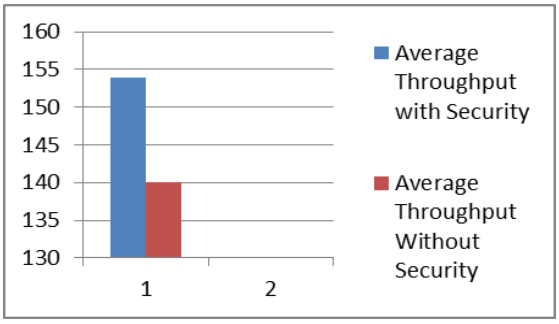


Fig. 5: Comparison of Average Throughput

This graph shows the average throughput comparison for network with key and without key. The average throughput has tremendously increased when key is used. More packets are being received at the destination when key is used.

Packet Delivery Ratio

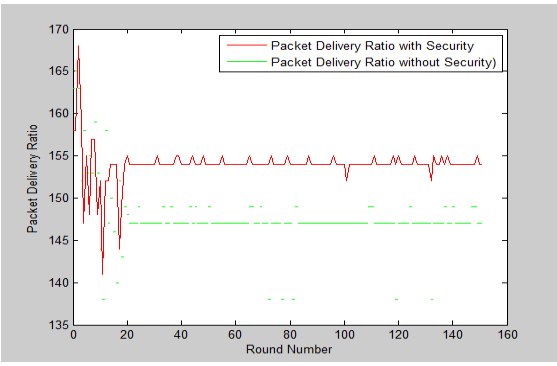


Fig. 6: Packet Delivery Ratio Comparison

This figure shows the packet delivery ratio for both the scenario that is packet delivery ratio with security and

packet delivery ratio without security. The packet delivery ration has shown the stability in case of enforcing security. But in case of maintaining no security the packet delivery shows large amount of fluctuation. So the network becomes more efficient while maintaining the security.

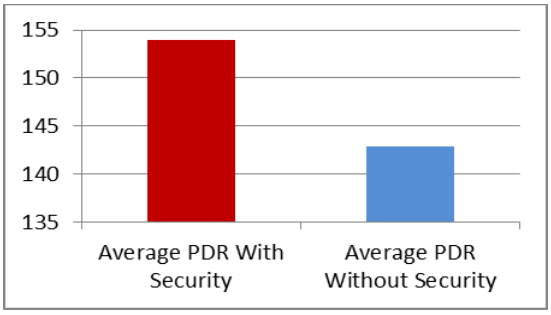


Fig. 7: Comparison of Average PDR

This graph shows the average packet delivery ratio for network with key and without key. More packets are being delivered from source to destination when network communication uses key.

Dead Node Count

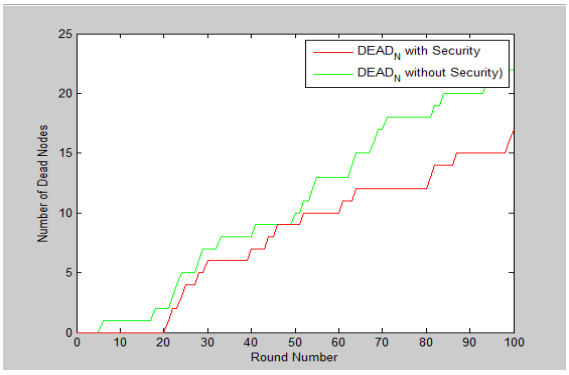


Fig. 8: Dead Node count comparison

This figure shows the dead node count comparison for network with security and network without security. It shows while maintaining the security less number of nodes will get dead. Even extra data is also exchanged for maintaining security. Less amount of energy is wasted due to insecurity in the network.

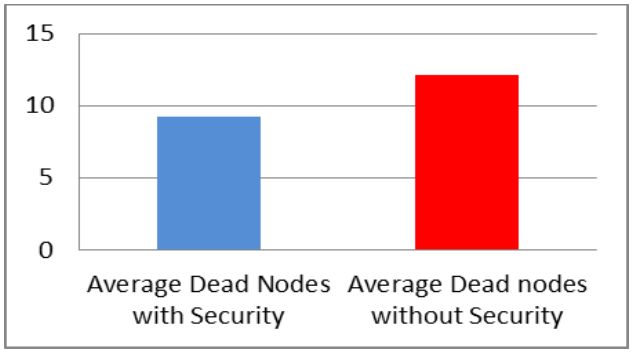


Fig. 9: Average Dead Nodes count graph

This graph shows the comparison of dead node count for both the situation when key is used and when key is not used. When key is used less number of dead nodes count is there. That means less number of nodes will deplete to zero energy.

Discussions

This whole system of implementing shows the difference between two cases one is network with no security and network with security. Network with security shows improvement in packet delivery ratio, Throughput, Dead node count, life time of the node. All the parameters have shown the improvement. By maintaining the security WSN has shown improvement in delivery of packets also it has shown the improvement in energy recovery.

Conclusion

WSN is wireless sensor network. It has various sensor nodes communicates to the base station for the collective data transmission. Base station will process this received data for further use. Each sensor node works in hierarchy of the nodes. Each sensor node communicates to the cluster head and cluster head to the base station. This base station or sink node can be stationary or mobile. This way communication is taken place. While communication there is the issue of maliciousness of the nodes. Sensor node or cluster head may works maliciously. Base station never knows whether data it is receiving is from the legitimate node or from the malicious node. So for making it ensure that data has been transmitted from the legitimate node each sensor node used RSA based public key. When this encrypted data will be received at the base station will be decrypted. It will helps in identification of malicious node. Because public key is shared by the base station to the legitimate node. No malicious node is having the ability to use public key. In this way by maintaining the security all the parameters like Packet delivery ratio, Dead node count, throughput, Life time of node has shown the improvement.

Future Work

In current research various aspects like WSN, KEYS etc. has been discussed. Using keys will enhance the security. So that malicious node cannot be the part of the communication. So further this research can be enhanced with energy saving security measures. In current research Asymmetric key has been used. This key is based on public and private key. Further another technique can be researched to decrease the load on the network.

References

1. Selva Reegan A, Baburaj E," Polynomial and multivariate mapping-based triple-key approach for secure key distribution in wireless sensor networks", Computers and Electrical Engineering 0 0 0 (2016) 1–17
2. Ze Wang, Maode Ma, Jigang Wu," Securing wireless mesh networks in a unified security framework with corruption-resilience", Computer Networks 56 (2012) 2981–2993
3. Omar Cheikhrouhou," Secure Group Communication in Wireless Sensor Networks: A survey", 25 January 2015.
4. Shio Kumar Singh 1, M P Singh 2, and D K Singh," Routing Protocols in Wireless Sensor Networks – A Survey", Vol.1, No.2, November 2010.
5. Anjali, Anshul Garg and Suhali,"Distance Adaptive Threshold Sensitive Energy Efficient Sensor Network (DAPTEEN) Protocol in WSN", 2015 International Conference on Signal Processing, Computing and Control (2015 ISPCC)

6. Pooja Chahal,Gaurav Kumar Tak,"Hybrid Protocol for Handling Security using SBPGP",Volume 115,pp. 40-50,2015.
7. Anju Chahal,Anuj Kumar,Auradha,"SECURE KEY MANAGEMENT IN AD-HOC NETWORK: A REVIEW",Vol. 7,pp. 1009-1017,2014.
8. Vandana Mohindru,Yashwant Singh,"Efficient Approach for Securing Message Communication in Wireless Sensor Networks from Node Clone Attack",Vol 9(32),2016.
9. Madhumita Panda,"Security in Wireless Sensor Networks using Cryptographic Techniques", Volume-03, pp-50-56, 2014.
10. Anup Ashok Patil,Shital Mali,"Hybrid Cryptography Mechanism for Securing Self-Organized Wireless Networks",vol. 3,2016.
11. Chitra Gupta,Priya Pathak,"Movement Based or Neighbor Based Tehnique For Preventing Wormhole Attack in MANET",vo. 4,pp-345-350,2016.