PROVIDING SECURITY FOR MULTIPATH ROUTING PROTOCOL IN WIRELESS SENSOR NETWORKS

K Renuka[1], G. Murali[2]

[1]*M. Tech, Computer Science and Engineering, JNTUA College of Engineering, Pulivendula, Andhra Pradesh, India*
[2]*Assistant Professor, Computer Science and Engineering, JNTUA College of Engineering, Pulivendula, Andhra Pradesh, India*

Abstract

Wireless Sensor Network (WSN) is a combined group of sensors form a network. WSN will monitor the changes in physical conditions and it will forward the data via multi hop network. Sensors are dynamic in nature so the lifetime of sensors and providing security for the data transmitted by the nodes are the major problems faced by the Wireless Sensor Networks (WSN). Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol is used for generating multiple paths between source and destination. Route discovery and route maintenance are main services of AOMDV. By having, Multipath routing protocol increases the lifetime of the sensors by distributing the traffic load among all the paths instead of single path in a network. The malicious node introduces many attacks on WSN because the network is dynamic in nature. The Warm Hole attack is one of the threat in which it will deviates the original path by introducing a tunnel between source and destination. Secure and authentic Multipath Routing Protocol in WSN is a major challenge and should be proposed which overcomes Warm Hole attack and maintain secure data transmission in the network. Elliptic curve cryptosystem (ECC) is used to prevent the attack and improve the performance of a sensor network by sharing secret keys among nodes in the network. By using Hop by Hop authentication scheme, the authentic message will be transmitted between source and destination in the Wireless Sensor Network. Performance evaluation will be done by using measures such as packet delivery ratio, end-to-end delay and throughput.

Keywords: *Wireless Sensor Network, Multipath Routing, AOMDV, Warm Hole attack, ECC*

----------***----------

1. INTRODUCTION

WSN contain sensors, which are small in size and more in number. These are operated in unattended environment such as pressure, temperature, etc. WSN used in many applications like military, home automation, controlling traffic and health care centers.

WSN operated in critical conditions with thousands of sensor node which are constrained in terms of energy, memory and communication. Because of these constrains, the reliability of WSN is low. So, due to these constraints, sensors may expire earlier than their lifetime. Every time the network is changing because of dynamic nature of WSN. Because of these characteristics, maintaining the network is also became a challenge.

Low Interference Energy Efficient Routing (LIEMRO) is a type of reactive routing protocol. It will find all the possible routes between source and destination, but excludes the property of node disjointness. The load balancing is done by considering parameters average interference level, average residual battery and Estimated Transmit Energy (ETX) for each path. It does not use the same path which one already used in the network, because this character will increase the number of Over Head. A novel AOMDV protocol used for selected data forwarding. It will provide same load in the entire path which are available on the network. It will consider the residual energy of the all nodes. Then it will choose a route for data forwarding. The route will change dynamically. Hop by hop authentication is a scheme authenticates every node in a network whether authorize or not.

Providing security is also a major challenge in Wireless Sensor Network and it is concentrates on maintain secure and authenticated data transmission between sensor nodes, used in many secured application like military and healthcare centers. The secure WSN obey all basic characteristics like availability, integrity, secrecy and confidentiality[1][2].

2. LITERATURE REVIEW

"Sensor Networks: An Overview" [1] has focuses on fundamentals and characteristics of sensors and also explains the challenges of sensor network. This paper include the architecture, working procedure and applications of sensor network.

Providing security for Multipath Routing Protocols by authentication will be explained in [2]. It contains working procedure of routing protocol and how the authentication will be provided for the Multipath Routing. [3] also includes functionalities about AOMDV protocol. The performance evaluation of AODV and AOMDV is explained in the paper[6].

[4] and [5] explains the Warm Hole attack and its consequences. These papers also explain the technique required for detection and prevention of Warm Hole attack will be explained in [4] and [5]. And also compare the Quality of service for each technique.

The importance of Elliptic Curve Cryptosystem and the creation of elliptic curves explained in [7]. This paper also includes algorithms of ECC. Generation and distribution of keys will be explained in [8].

[9] explain about public key cryptography and also include Elliptic Curve Discrete logarithm problem and examples of elliptic cryptography.

3. ADHOC ON-DEMAND MULTIPATH DISTANCE VECTOR ROUTING (AOMDV) PROTOCOL

AOMDV is a multipath routing protocol and it is an extension of Ad hoc On-demand Distance Vector (AODV) routing protocol.

AODV establishes a single path between source and destination. If any route fails, it is not possible to reconfigure the route immediately. So, secure data transmission is not possible with AODV protocol and hackers can easily get the routing information.

AOMDV protocol offers multiple paths for sending the data instead of single optimal path. It is easily reconfigure the failure path immediately by selecting another route from multiple paths. It will distribute the load equally among all the paths available in the network. Efficiently, AOMDV reduces the packet delay and also packet loss [2].

3.1 Working of AOMDV

If the source has no route to the destination sensor, then source initiates the route discovery in an on demand fashion. After generating RREQ, node looks up its own neighbor table to find if it has any closer neighbor sensor toward the destination sensor. If a closer neighbor sensor is available, the RREQ packet is forwarded to that sensor. If no closer neighbour sensor is the RREQ packet is flooded to all neighbour sensors. A destination sensor replies to a received RREQ packet with a route reply (RREP) packet.

Rout discovery and Route maintenance are the main services of AOMDV. Here, every RREQ is being considered by source node for route discovery. Every node maintains a route entry table which contains a list of next hop and advertised hop count for the destination. By using this hop count the alternative paths will be discovered by the source node[2] [3][6].

4. WARM HOLE ATTACK

Warm hole attack is one of the severe attacks in wireless sensor networks. It needs two or more opponents have better communication resources than original nodes and establish a better channel between them. The attacker stores the packet information at one location, and tunnels them into another location.

In the below figure A and B represents the source and destination nodes, X and Y represents warm hole nodes respectively.

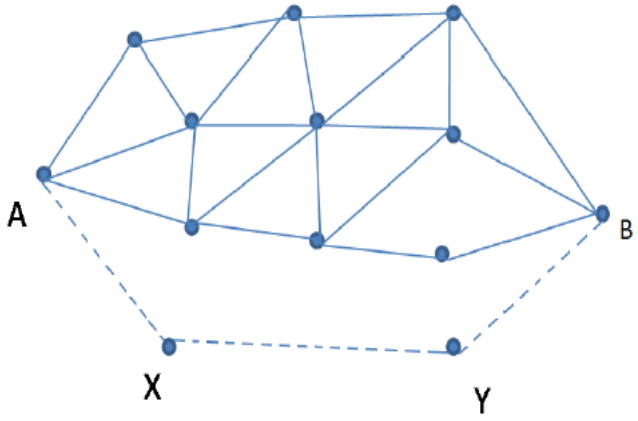

Fig-1: Warm Hole attack

Actually, the information from source to destination routes among the normal nodes but here the attacker can makes a tunnel between source and destination by introducing warm hole nodes.

Warm hole attack can be propelled using some modes like encapsulation, out of band channel, high power transmission and protocol deviation.

This creates some effects on sensor network such as routing false information, network topology changes, packet damage, packet alter by warm hole nodes and changes the message stream [4].

Warm Hole attack is detected by considering the following terms:
1) Strength: It is amount of traffic attracted by wrong link announced by the colluding nodes.
2) Length: There is a difference between the actual path and advertised path, more anomalies will be detected.
3) Attraction: This term refers to the reduction in path length offered by the worm hole [5].

5. ELLIPTIC CURVE CRYPTO SYSTEM

Elliptic Curve Cryptosystem (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create smaller, faster and more efficient cryptographic keys.

For encryption of data it uses public key and distribute this key to all nodes in the network. The private key is used for decryption of data at destination node. ECC shares low weight keys in a network. The elliptic curve consists of numbers (x, y) known as points which satisfies the equation $y^2=x^3+ax+b$. Here a and b represents elliptic curves.

The technique will be shown in below figure:

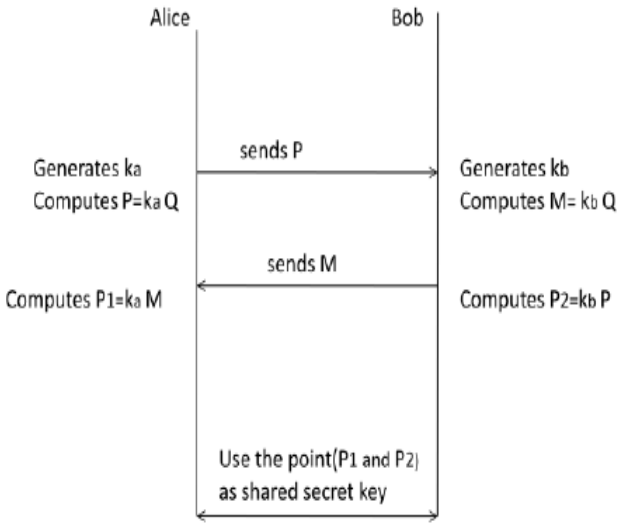

Fig-2: distribution of secret keys

In Fig-2, Alice generates a key ka and computes point P by using point Q. In the same way Bob also generate a key kb and computes point Q. Later, both are exchanges their points and then compute point P1 and P2. These computed points used as shared secret keys. By sharing of keys, the destination will know the source clearly so the messages received from false nodes will be ignored. ECC concentrates on generating elliptic curves by using points, which evaluates the wireless sensor network.

Alice and Bob know both secret keys. If any attacker wants to get the data then hacking of data will be more difficult because the secret key does not match. So, illegal request of data will be discarded. This technique provides the security for the sensor network and also improves the performance [7].

6. PROPOSED SYSTEM

A sequence of steps to detection and prevention of warm hole attack in wireless sensor network is shown in the below Fig-3.

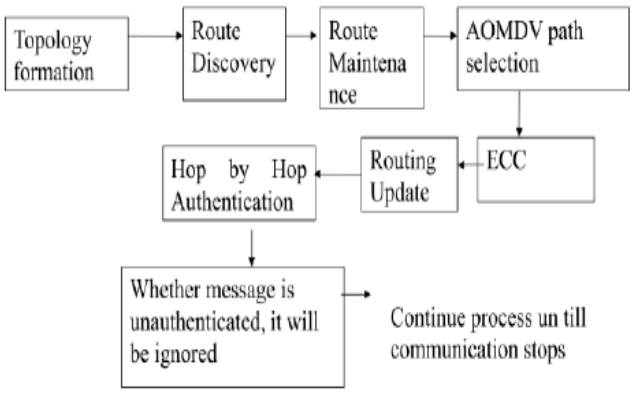

Fig-3: flow chart of proposed system

In Fig-3, first establishes the topology and discover all feasible routes between source and destination. Path selection will be done using AOMDV protocol. The protocol finds multiple paths between source and destination. If any route fails, then the other route will be taken immediately for data transmission. By using ECC distributes the keys among nodes in the sensor network.

The data will be encrypted and decrypted by using public and private keys. So, each node will know about all the nodes in the sensor network because every node maintains the route entry table. Hop by Hop authentication will be done for secure data transmission. If the data is authentic then it will be forwarded otherwise the message will be discarded. This process will be continued until the communication stops. By authenticate each node easily avoid the attacks in the network.

7. RESULT ANALYSIS

The analysis of results will be done by using metrics like Packet Loss, Packet Delivery Ratio (PDR), Throughput and End-to-End Delay.

Packet Delivery Ratio: The ratio of the number of delivered data packets to the destination.

Throughput (bits/sec): Number of packets received per simulation time

End-to-end Delay (sec): The average time taken by a data packet to arrive in the destination.

Table-1: calculation of metrics

Metrics	Warm Hole attack	ECC
Packets sent	1123	1123
Packets Receive	819	1098
Packet Loss	304	25
PDR	72.92	97.77
Throughput	105988	119828
End-to-End Delay	0.0824	0.1416

In Table-1, calculate the metrics for a network after attacking the Warm Hole and after applying ECC scheme. Clearly, ECC shows the better result as increase in the PDR and Throughput.

Fig-4 is the graph representation for the above results shown in the Table1.

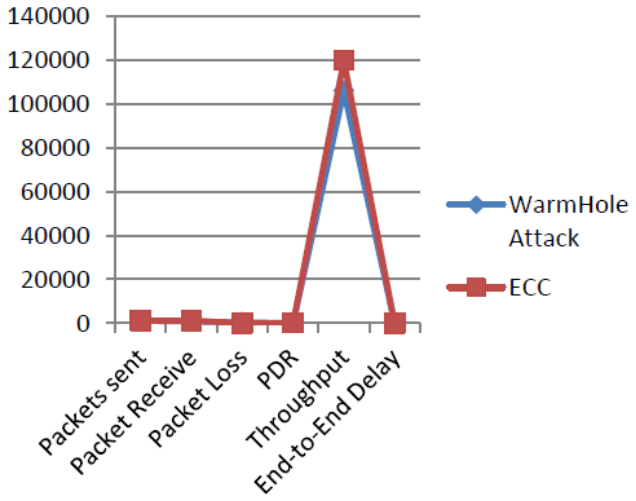

Fig-4: comparision of warmhole attack and ECC

8. CONCLUSION

Wireless sensor networks can easily get a wide range of several attacks because of their dynamic nature and positioning in open and critical environment. This paper focuses on security of the network. Many researches develop many techniques but not any technique can prevent all the attacks. Therefore, finding such network which overcomes many attacks is still a challenge.

REFERENCES

[1]. S.Madria, M.Tubaishat, "Sensor Networks : An Overview", IEEE, April/May 2013.
[2]. Gaurav Gulhane, Nikita V.Mahajan, "Securing Multipath Routing Protocol using Authentication approach for Wireless Sensor Network" DOI 10.1109/CSNT.2014.153 IEEE.
[3]. Mahesh K Marina, Samir R Das "Ad hoc ondemand multipath distance vector routing" DOI 10.1002/wcm.432, 2006.
[4]. Akanksha Gupta, Anuj K.Gupta "A Survey: Detection and Prevention of warm hole attack in wireless sensor network" ISSN: 0975-4172, Vol 14, 2014.
[5]. Jyothi Thalor, Ms Mounika," Warm Hole Attack Detection and Prevention Technique in Mobile Adhoc Networks: A Review" Vol 3, ISSN: 2277 128X, Feb 2013.
[6]. K.Vanaja, "An Analysis of Single Path AODV vs Multipath AOMDV on Link Break using Ns2" ISSN-2277-1956.
[7]. Florian Rienhardt ,"Introduction to Elliptic curve Cryptography" , 2013.
[8]. Dragan Vidakovic, DuskoParezanovic, "Generating Keys in Elliptic Curve Cryptosystem", ISSN: 1694-2108 | Vol. 4, No. 1. August 2013.
[9]. Elaine Brow, "Elliptic Curve Cryptography", Math 189A, December 2013.