ISSN:0975-9646

Vampire Attacks Deploying Resources in Wireless Sensor Networks

P.Rajipriyadharshini[1],V.Venkatakrishnan[2],S.Suganya[3],A.Masanam[4]

[1,3,4]*M.E,Computer science and Engineering,*
Parisutham Institute of Technology and Science,Tamilnadu,India.
[2]*Assistant professor,Information Technology,*
Parisutham Institute of Technology and Science,Tamilnadu,India.

Abstract Wireless sensor network is a communication network across the sensors nodes. Sensor nodes collects information about the physical environment. Now-a-days one main issue in wireless adhoc sensor network is wastage of energy at each sensor nodes. Energy is the one most important factor while considering sensor nodes. Wireless sensor networks requires solution for conserving energy level. One new type of attack called vampire attack, which occurring at network layer. It leads to resource depletion (energy) at each sensor nodes, by destroying battery power of any node. It transmit a small complaint messages to disable a whole network, hence it is very difficult to detect and prevent. Existing protocols are not focusing on this vampire attack happening on routing layer , hence there exist two types of attacks namely, carosuel and stretch attack. Hence there is a large of energy loss. New protocol called PLGP, a valuable and secure protocol is proposed along with the key management protocol called Elliptic Diffie-Hellman key exchange protocol to avoid this vampire attack. By using this, existing problems can be overcome.

Keywords – wireless sensor networks,vampire attack, resource consumption,encryption,decryption,security.

I. INTRODUCTION

1.1.Wireless Sensor Networks:

Sensor network is composed of a large number of sensor nodes that are deployed in a wide area with very low powered sensor nodes. The wireless sensor networks can be utilized in a various information and telecommunications applications. The sensor nodes are very small devices with wireless communication capability, which can collect information about sound, light, motion, temperature etc and processed different sensed information and transfers it to the other nodes. The following figure-01 illustrated the Wireless Sensor Network scenario.

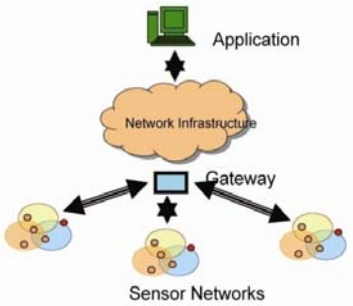


Figure 1.1.wireless sensor network

1.2. Characteristics of WSN

Wireless Sensor Networks are:

- Short-range broadcast communication and multihop routing
- Dense deployment and cooperative effort of sensor nodes
- Frequently changing topology due to fading and node failures
- Severe limitations in energy capacity, computing power, memory, and transmit power.

1.3. Vampire Attacks

Vampire attacks are most popular attack in networks ,it is the composition and transmission of a message that causes more energy to be consumed by the network, than if an honest node transmitted a message of identical size to the same destination. By using PLGP the effect of this vampire attacks are reduced.

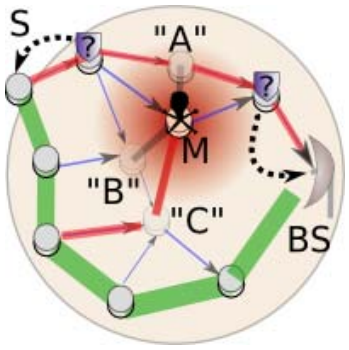


Figure 1.2. scenario of vampire attack

This paper first, evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks. Second, shows simulation results quantifying the performance of several representative protocols in the presence of a single Vampire (insider adversary).Third, modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

In PLGP, forwarding nodes do not know what path a packet can took .If the path is known, it will allow the adversaries to divert the packet from any part of the network. The PLGP avoids Vampire attacks during the packet forwarding phase. The information available to the honest node is its own address and the packet destination address. By knowing the previous hop information the attack levels are raised, so to rectify it and reduce the attack the PLGP method is used.

II. EXISTING SYSTEM

In Routing layer, the exhaustion attacks are not thoroughly analyzed. A malicious user may interact with a node in an otherwise legitimate way, but for no other purpose than to consume its battery energy. Battery life is the critical parameter for many portable devices. Existing work on secure routing attempts to ensure that adversaries cannot cause path discovery to return an invalid network path.

PLGP consists of two phases, i)Topology discovery phase ii)Forwarding phase.*Topology discovery* – it forms a group of

nodes by broadcasting unique ID.*Forwarding phase* - all decisions are made independently by each node. When receiving a packet, a node determines the next hop by finding the most significant bit of its address that differs from the message originator's address.

2.1. CLASSIFICATION OF ATTACKS –

Stretch attack - Stretch attack, since it increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. In this attack, adversary causes packet to travel long distance than the needed to reach the destination leading to energy wastage. Thus both lead to consumption of energy unnecessarily.

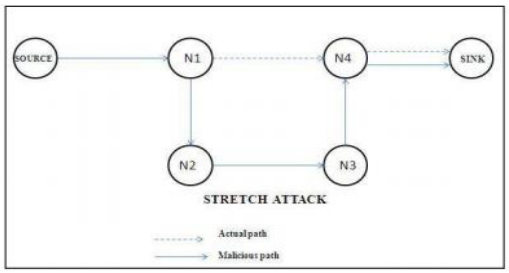


Figure 2.1.Stretch attack

Carousel attack - In this attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. In this malicious node introduces loop in the path of packet travel purposely to drain the energy of honest nodes.

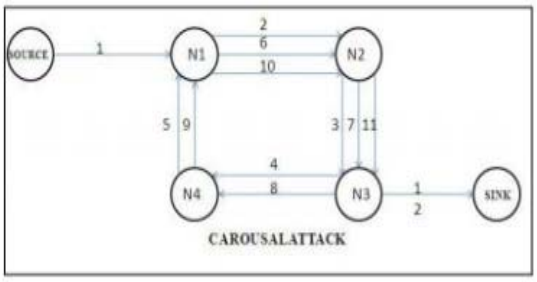


Figure 2.2.Carosuel attack

III.PROPOSED SYSTEM

Modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding,by using PLGP.It consist of Topology discovery phase,to ensure the current information or status of the topologies. PLGP implies no backtracking. Modify the forwarding phase of PLGP by key management scheme, Elliptic Curve Cryptography(ECC) by encrypting and decrypting the transferring message.

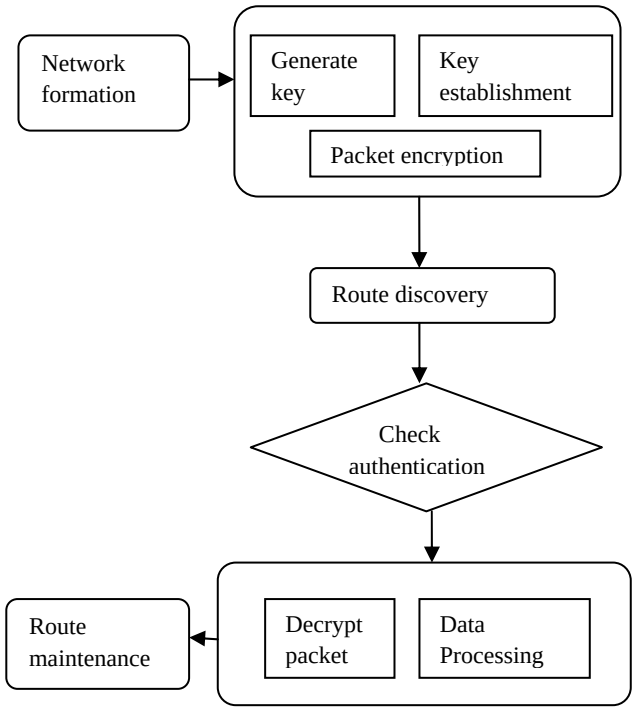
3.1.Algorithm : In this paper, ECDH algorithm is used for secure and reliable data transfer. The algorithm goes secure forwarding of packet to destination posture of the node. It consist of the following steps,*Key Generation, Key Exchange, Encryption/Decryption.*

A)Key generation : Consider A needs to send a message to B, i)A generates its private key nA and calculates its public key , PA= nA * P. ii) B generates its private key nB and calculates its public key , PB= nB * P.

B)Key Exchange : A computes it's shared key , k=nA * PB.B computes it's shared key , k=nB * PA.

C)Encryption/Decryption :A sends c_m (2 cipher texts=kG,P_m + kP_B) and B decrypt the message using different shared key.

3.2.Architecture diagram : Initially the wireless network is formed,by postioning the nodes. Generation of keys and the key is established by using the Elliptic Diffie-Hellmann key exchange algorithm.



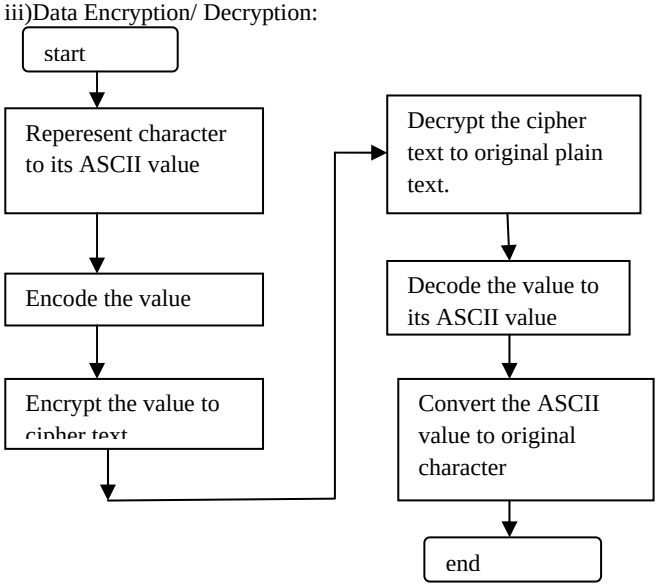
Authentication is checked between the nodes. The encryption and decryption of the message also done by ECC algorithm. Finally the discovered route is maintained in the network.

3.3. Modules : Several set of modules were developed for making that nodes and exchanging the keys between them for secure data transfer. The modules are *i)Network Formation ii)Key Establishment iii)Data Encryption/ Decryption iv)Route maintenance.*

i)Network formation : Formation of network- forms a group of nodes.

ii)Key Establishment : Sender and Receiver want to agree on a shared key.

iii)Data Encryption/ Decryption:



iv)Route maintanence: Route maintenance performed only while route is in use.

IV. IMPLEMENTATION TOOLS

NS-2 is n event driven packet level network simulator developed as a part of the VINT project (Virtual Internet Test bed).Version 1 of NS was developed in 1995 and with version 2 in 1996 Ns-2 with C++/OTCL integration feature. Version 2 included a scripting language called Object oriented Tcl (OTCl). It is an open source software package available for both Windows 32 and Linux platforms. NS-2 has many and expanding uses included.

- To evaluate that performance of existing network protocols
- To evaluate new network protocols before use.
- To run large scale experiments not possible in real experiments
- To simulate a variety of ip networks.
-

SOFTWARE TOOLS USED WITH NS-2

In the simulation, there are the two tools are used.

NAM(Network Animator)

xGraph

NAM (Network Animator)

NAM provides a visual interpretation of the network topology created. The application was developed as part of the VINT project. Its feature is as follows,Provides a visual interpretation of the network created,Can be executed directly from a Tcl script,Controls include play; stop fast forward, rewind, pause, a display speed controller button and a packet monitor facility.,Presented information such as throughput, number packets on each link.

X Graph

X- Graph is an X-Window application that includes:

Interactive plotting and graphing Animated and derivatives To use Graph in NS-2 the executable can be called within a TCL script. This will then load a graph displaying the information visually displaying the information of the file produced from the simulation. The output is a graph of size 800 x 400 displaying information on the traffic flow and time.

V.CONCLUSION

A new class of resource consumption attacks (vampire) that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes battery power.This attack is mitigated by proposing a key management protocol, Elliptic Diffie-Hellman key exchange protocol.

REFERENCES

1. A. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography” CRC Press, 1996.
2. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly secure key distribution for dynamic conferences. In Information and Computation, 146 (1), 1998, pp 1-23.
3. D. Liu, P. Ning, Establishing Pairwise Keys in Distributed Sensor Networks, 10th ACM CCS '03, Washington D.C., October, 2003
4. D.B. Johnson, D.A. Maltz, and J. Broch, “DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks,”Ad Hoc Networking, Addison-Wesley, 2001.
5. E. Y. Vasserman, N. Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks," vol. 12, Feb. 2013.
6. G. Gaubatz, J.Kaps, B. Sunar Public Key Cryptography in Sensor Networks – Revisited. 1st European Workshop on Security in Ad-Hoc and Sensor Networks
7. G. Jolly, M. Kusçu, P. Kokate, M. Younis. A Low-Energy Key Management Protocol for Wireless Sensor Networks. Eighth IEEE International Symposium on Computers and Communications
8. Joel H. Spencer, “The Strange Logic of Random Graphs”.
9. M. Bellare, P. Rogaway , “Introduction to Modern Cryptography” , November 3, 2003
10. R.C. Shah and J.M. Rabaey, “Energy Aware Routing for Low Energy Ad Hoc Sensor Networks,” Proc. IEEE Wireless Comm. And Network Conf. (WCNC), 2002.

BIOGRAPHIES

[1]P.Rajipriyadharshini, received B.E(computer science) Degree from Anna university,Chennai and now pursuing M.E(computer science and engineering) in Parisutham Institute of technology andscience,Thanjavur,Tamilnadu,India. Interested in mobile computing,networking.

[2]V.Venkatakrishnan,received M.Tech degree from Anna university,Chennai.He is an Assistant professor in Parisutham Institute of technologyandscience,Thanjavur,Tamilnadu,India.He is interested in Networks, mobile computing.

[3]S.Suganya, received B.E(computer science) Degree from Anna university,Chennai and now pursuing M.E(computer science and engineering) in Parisutham Institute of technology andscience,Thanjavur,Tamilnadu,India. Interested in Cloud computing, Database management.

[4]A.Masanam, received B.E(computer science) Degree from Anna university,Chennai and now pursuing M.E(computer science and engineering) in Parisutham Institute of technology andscience,Thanjavur,Tamilnadu,India. Interested in mobile computing,networking.