Cluster Head Creation to Overcome Vampire Attack

Anjali Nair[1] Anu Maria Sebastian[2] Divya T Sunny[3]
[1,2,3]Department of Computer Science
[1,2,3]SJCET Palai

Abstract— As an emerging platform wireless Adhoc sensor network emerged in the field of remote sensing data assessment, analysis. Today network plays main role in one's life mainly communication take place through this network so network security is one of the main concern. The security work in this area is mainly focusing over denial of communication at the routing or medium access control level. Network survivability is one of the main concerns. It reduces the battery power of the network hence one cannot send message through that network for the desired time it will be expensive to use new battery. In this paper we are trying to reduce this kind of attack in wireless sensor network by using cluster mechanism. Here we are using MOCA(Multiple over lapping cluster Algorithm)it create new cluster in each desired or valid route.

Key words: Ad-Hoc Network, Cluster, Cluster Head, MOCA, Heed, Leach, Vampire Attack, Wireless Sensor Network

I. INTRODUCTION

WIRELESS Sensor Network (WSN) can be defined as a network, which communicates wirelessly following an ad hoc configuration using small embedded devices, called sensors. Sensor network are used to measure the environment and send the information. These network are mainly consist of many nodes in which some of the nodes are sensor nodes these nodes use to communicate by broadcasting the message. Mainly This type of network are used in military surveillance to monitor enemies activity. This network survivability depends upon the lifetime of battery. Nodes position may vary as the battery life gets depleted then that node will be of no use so its position may change that's why nodes are autonomous and will be disregarded. Have only limited power, low computational capabilities and limited memory. One of the main issues that should be studied in WSNs is their scalability feature, their connection strategy for communication.

Wireless network is mainly used for the everyday functioning of people and organization so one cannot tolerate fault as lack of availability may cause business failure & lost productivity. Mainly WSN are vulnerable to denial of service attack because of ad-hoc network organization. Sensor is usually depend upon the battery power. One of its main disadvantages is idle consumption of energy. Here loss of packet may appear because of packet collusion as the same packets were send by a particular id to a particular node repeatedly causing it engage for long time. This wireless sensor network are highly deployed and can be reconfigured it is highly robust due to their distributed nature node redundancy & lack of single point failure is another reason.

Mainly there are two type of attacks short term denial of service attack and long term denial of service attack. Mainly Security measures are taken for short term denial of service attack these attack are denial of communication or service attack in Adhoc network or WSN mainly these sort of attack are mitigated using many methods while permanent denial of service attack are not concentrated that much but for continuous message transferring one require network survivability as the battery is used as a source of energy for the network there are more chances of depleting energy at the time of long distance communication and when unwanted messages are sent from a node or from a particular id causing the nodes energy to depleted. This kind of attack no effective methods are discovered till now. One of this sort of permanent attack is vampire attack. Vampire attack is a resource depletion attack it use to drain battery life these attack are not specific to any protocol it mainly depend upon the routing protocol. Here the worm try to pass the message among the node which is not participating in communication and may be a malicious node .The intension of this sort of node is to deplete battery life of the node and soon to get depleted. It's very hard to mitigate this sort of attack from network. It is a sort of permanent denial of service attack. Many works were done to mitigate this attack but not able to completely mitigate it. It is independent of design or particular routing protocol.

II. EXISTING SYSTEM

Many resource depletion attacks are there sleep deprivation torture & denial of sleep attack are few. Sleep deprivation blocking the node to enter low power sleep state thus making its power to be drain faster. Denial of sleep attack are mainly at MAC layer, mostly work are considered on minimal energy routing protocol which tries to increase malicious node make the minimal routing protocol as the attack will produce a route. One of the existing secure protocol SEAD(Secure Efficient Distance vector)this is mainly used against removing carousel attack where attacker tries to create the loop of messages delivered so it may be possible that it take a maximum time to send a packet to destination. If it consumes much time & cause delay to judge the most significant hop. To avoid such situation use cluster head among the nodes. Loose Source Routing is first preservation mechanism the forwarding nodes are able to route the packet if know the shortest path to destination. Denial of service attack mainly concentrate towards MAC layer and data confidentiality. In sensor network there is lack of security & privacy. Forward packet algorithm prevents vampire attack but does not overcome completely. Here malicious node can send protocol complaint message and reduce battery power.

A. AODV Mechanism

Routing is done from the source node to the destination node. This causes the large amount of energy to be used. The energy wastage of transmitting & receiving packet to appropriate destination .it is on demand distance vector protocol here multicast routing take place. In routing table IP addresses and sequence number of the group are stored. Destination sequenced distance protocol is one of the

property of distance routing protocol. It is table driven protocol. It store initial state and destination vector.

B. Eliptic Curve Cryptography

Public key cryptosystem just like RSA. Run Length Algorithm It's a very simple method of data compression.

C. Cluster Formation

Leach Mechanism CH is selected where they use to communicate .Attack can be prevented & overall threshold value is to be known to elect a clusterhead .cluster group members are having same energy level this is a hierarchical network. One of the drawbacks is clusterhead elected randomly.

1) Disadvantage of Existing System

- Power Outages
- Due to environmental disaster loss in the information.
- Loss in productivity
- Various DOS attack
- Secure level is low

III. PROBLEM DESCRIPTION

Malicious node the unwanted node plays the main role in vampire attack this malicious node while routing come between the source node and the destination node and send the packet to any other node inspite of the required node. This malicious node pass the message to a particular node for many times making network down

IV. PROPOSED SYSTEM

Nodes Energy can be preserved by using cluster formation mechanism. Cluster is a group of certain nodes where any of the node among the cluster is selected as the cluster head node. Cluster head is selected from the group which satisfy the required condition this cluster head participate in transferring messages from one cluster to another cluster this mechanism preserves the energy of the network by participating or making the require node to be active at the time of transmission .many cluster forming methods are there among them we are using MOCA mechanism which create multiple overlapping clusterhead. This method is much better than leach mechanism as here inter cluster routing will take place. In this method node localization is done. Recovery from CH failure. This mechanism have distributed clusterhead using this mechanism get dynamic cluster head according to the energy of the node select the clusterhead from the group whereas it uses the property of heed too where clusterhead is again selected using the residual energy left. It also uses the concept of leach algorithm threshold value. A certain value is considered to be the trust value if the node is having that much energy then it will be selected as the clusterhead but it does not have dynamic clusterhead creation mechanism where as we use MOCA mechanism an effective method.

V. CONCLUSION

In this paper we try to mitigate vampire attack using overlapping cluster head selection mechanism. A detailed study of existing cluster protocol is done in wireless sensor network. We use here broadcasting technique and moca protocol to mitigate the energy depletion attack in network moca uses the combination of both heed and leach protocol whereas it is having a k-hop cluster topology. Using moca obtain the node with highest energy one more parameter for moca is residual energy.

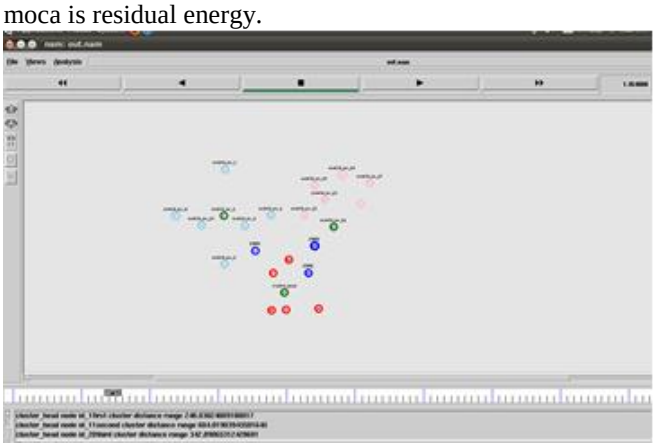

Fig. 1: Cluster Head Creation

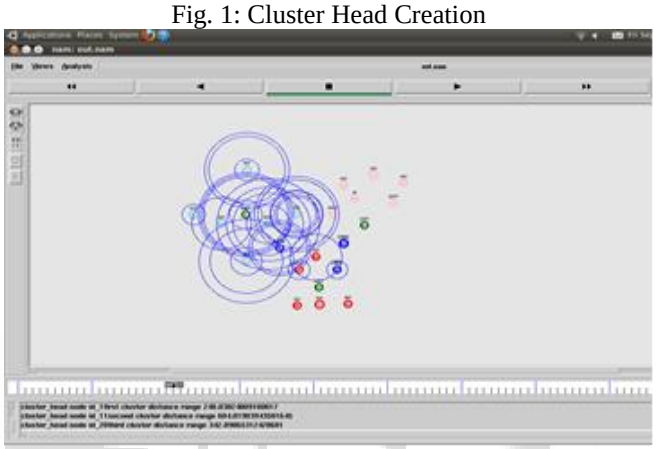

Fig. 2: Residual Energy of Cluster Nodes

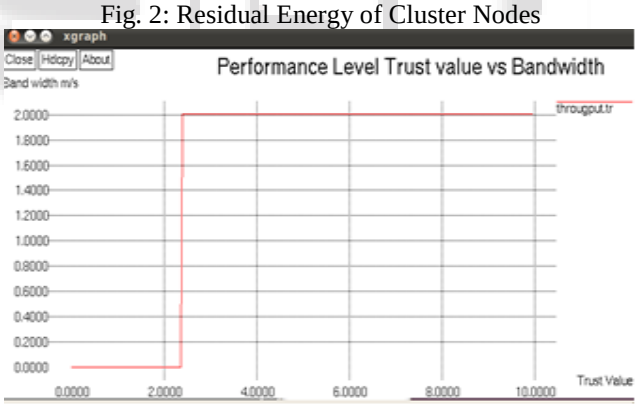

Fig. 3: Performance Evaluation

REFERENCES

[1] Sharmila, V., and Mr K. MuthuRamalingam. "Energy Depletion Attacks: Detecting and Blocking in Wireless Sensor Network." International Journal of Computer Science and Mobile Computing 3.8 (2014): 100-109.

[2] Eugene Y. Vasserman and Nicholas Hopper, "VampireAt-tacks: Draining Life from Wireless Ad Hoc Sensor Net-works", IEEE Transactions on Mobile Computing,Vol. 12, No. 2, February 2013.

[3] Korkmaz T.; "Verifying Physical Presence of Neighbours against Replay-based Attacks in Wireless Ad Hoc Networks"; Proc. International Conference on Information Technology: Coding and Computing 2005, ITCC 2005, pp. 704-709, 2005

[4] Eugene Y.Vasserman and Nicholas Hopper, "Vampire at-tacks: Draining life from wireless ad-hoc sensor networks" (2013).
[5] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Net-works," Proc.IEEE INFOCOM, 2003.
[6] Virmani, Deepali, Akshay Jain, Ankit Khandelwal, Divik Gupta, and Nitin Garg. "Dynamic Clustering Protocol for Data Forwarding in Wireless Sensor Networks." arXiv pre-print arXiv:1306.1408 (2013).
[7] Gamwarige, Sankalpa, and E. Kulasekere. "An algorithm for energy driven cluster head rotation in a distributed wireless sensor network." In Proceedings of the international confer-ence on information and automation, pp. 354-359.
[8] Handy, M. J., Marc Haase, and Dirk Timmermann. "Low energy adaptive clustering hierarchy with deterministic clus-ter-head selection." In Mobile and Wireless Communications Network, 2002. 4th International Workshop on, pp. 368-372. IEEE, 2002K.
[9] N.M. Abdul Latiff, C.C. Tsimenidis, and B.S. Sharif, Energy-aware clustering for wireless sensor networks using particle swarm optimization, in IEEE Intl. Symposium
[10] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Trans. Vehicular Technology, vol. 58, no. 1, pp. 367-380, Jan. 2009..
[11] Y. Xu and H. Qi, Decentralized reactive clustering for col-laborative processing in sensor networks, in Proceedings of the 10th International Conference on Parallel and Distributed Systems (ICPADS'2004), pp. 54–61, July 2004.
[12] S. Selvakennedy, S. Sinnappan, and Y. Shang, A biological-ly inspired clustering protocol for wireless sensor networks, Computer Communications 30, 2786–2801,2007.
[13] Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks," Computer Comm., vol. 29, no. 2, pp. 216-230, 2006.
[14] D.R. Raymond and S.F. Midkiff, "Denial-of- Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, pp. 74-81, Jan.-Mar. 2008.

