ISSN 2319 - 5975

Volume 8, No.3, April - May 2019
International Journal of Networks and Systems
Available Online at http://www.warse.org/IJNS/static/pdf/file/ijns06832019.pdf
https://doi.org/10.30534/ijns/2019/06832019

An Energy Aware Fuzzy Approach for the Enhancement of WSN

Anjali V Nair[1], AjeeshS[2], Smita C Thomas[3]
Mount Zion College of Engineering, Pathanamthitta, India, vanju1020@gmail.com
Mount Zion College of Engineering, Pathanamthitta, India, ajeesh.s3@gmail.com
Mount Zion College of Engineering, Pathanamthitta, India, smitabejoy@gmail.com

ABSTRACT

Wireless sensor network refers to a group of spatially dispersed and dedicated sensors.Mainly used for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location.The lifetime enhancement of this network is a crucial factor while we designing a network.This is mainly because the powersource of each node is a small battery this is not replaced and recharged. Energy is an important factor for sensor node, while there is one new type of attack called vampire attack has been discovered which disables network by consuming battery life of sensor network.Proposed methodology supposed to provide dynamic detection and removal of vampire attack from WSN. According to the proposed solution vampire attacker will be detected on the basis of packet monitoring and violation of certain network rules among network nodes.

Key words-Wireless Sensor Network, Cluster Head

1. INTRODUCTION

Wireless sensor network is a one main issue in wireless ad-hoc sensor network is wastage of energy at each sensor nodes. Energy is the one most important factor while considering sensor nodes. Wireless sensor networks require solution for conserving energy level. One new type of attack called vampire attacks, which occurring at network layer. It leads to resource depletion (energy) at each sensor nodes, by destroying battery power of any node. It transmits 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, carousel and stretch attack. Hence there is a large of energy loss.In carousal 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**.**Another attack in the same vein isthestretch attack, where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes.As expected, the carousel attack causes excessive energy usage for a few nodes, since only nodes along a shorter path are affected.

In contrast, the stretch attack shows more uniform energy consumption for all nodes in the network, since it lengthens the route, causing more nodes to process the packet. While both attacks significantly network-wide energy usage, individual nodes are also noticeably affected with some losing almost 10 percentage of their total energy reserve per message.In order to overcome this energy efficiency problem here we proposed technique is rule based technique through packet header and data monitoring. This is not based on algorithmic approach it is a rule based approach. The energy is more used by each node when a packet loss is occurred in network. If a system A want to communicate with system B then that packet is not reached B and A did not get any acknowledgement from B. Then A again re send the data again and again. This will lead to over usage of energy by each node.

This is done by a malicious node. If vampire attack is present this will cause energy consumptions.Vampire attack happens in the network in the sense, any of the nodes in the network which is affected or infected and this nodes behaviour is abruptly changing for the network behaviour, this kind of nodes are called “Malicious node”. If malicious nodes present in the network energy that have been using by each and every nodes will increases drastically. The malicious node has been place in the network uniquely. First In between the routing nodes, and the second placed in the Source node itself. The chance of placing a malicious node in the routing path this makes causing damage in network. This Dissertation is mainly concentrates on the identification and avoidance of the malicious node.

Problems identified in the case of vampire attacks:
1) Improving network Lifetime
2) Route Optimality
3) A path to forward the packets by consuming less

energy.i.e. Maximum energy efficiency.

2. LITERATURE REVIEW

Miss V Subha and Mrs P Selvi [1] introduced defenses against some of the forwarding-phase attacks and described VSP, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. The proposed system introduces a novel authentication and key management mechanism called Hybrid Key Management. It is robust and scalable under limited memory constraints. It ensures strong security guarantees by using Low Power Routing (RPL).The proposed system avoids vampire attack by Elliptic curve Diffie-Hellman algorithm for authentication and Modified RSA algorithm for data Encryption.

A.Vincy, V.Uma Devi [4] proposed approach consists of two phases. In the first, phase detecting and preventing denial of service attack based on secret sharing(SS) algorithm. In the second phase, increasing network lifetime based on switching the node states. The data verification process is provided at both the server and client side. It provides comparatively high security. It reduced the intruder spoofing.

DeepmalaVerma, Gajendra Singh, KailashPatidar [3] suggested that work an internal attack namely vampire attack is investigated and an appropriate method is proposed for implementation and improving security with the performance of network.

AvulaSrikanth, R.V.Kishore Kumar [4] introduced Low configured wireless PDA's become a part of human life in the format of mobiles, sensors, cameras and other small digital electronic components. Due to the mobility and on-demand connectivity security is the major concern in this area always. Former researches on this area were concerned only on secured communications, medium access control levels. Apart from the general attacks at protocol level and data access level, recently PDA's encountered the problems of "Vampire Attacks" which damage the system by draining the batteries quickly.

S.K Das in [5] developed and proposed a non uniform node distribution strategy which achieves minimum balanced depletion. The energy aware routing in Rana et al. presented an A* algorithm based Energy Efficient Routing (ASEER) protocol to find optimal route in order to extend network lifetime [12]. In addition to 'h(n)' estimated and cost-so-far 'g(n)', ASEER's heuristic function introduces a new metric 'l(n)' that denotes the path cost count of weak nodes having less energy.

Delay aware energy balanced dynamic routing protocol by N.kaleswari and Dr k. Baskaran [6] proposed three phases, which finds the shortest path /best energy balanced based delay minimum optimal route. In the second phase alternate shortest path will be updated in the route table. This phase updates the new route if the working route is getting down.

Jae-Hwan Chang and Lindros Tassiulas[7] had extended the maximum lifetime routing problem to include the energy consumption at the receivers during reception.In wireless sensor networks where nodes operate on limited battery energy, the efficient utilization of the energy is very important. One of the main characteristics of these networks is that the transmission power consumption is closely coupled with the route selection. The energy efficiency has been considered in wireless adhoc network routing, but the conventional routing objective was to minimize the total consumed energy in reaching the destination.

Eugene Y. Vasserman (Vasserman et al.,[2] [8]) defined Vampire attacks, an attack which drains energy of network node and makes wireless network permanently disable. They have plot random topology of 30 nodes and created some malicious node and proved that this attack is vulnerable to various routing protocols. Work included study of various ways of vampire attacks for various types of protocols. Solution provided in this paper is PLGP which is proved first solution against vampire attack in packet forwarding phase of network communication.

3. EXISTING SYSTEM

In existing system as shown in figure 1, the header part of the data is checked to find the attacks.The data is accepted from different port and if any packet is loss in network means that is bouncing.We calculate the number of bounce packet,ds if it is in increased level means that IP is malicious node. In this way we identify the malicious IP.Here only data part is checked.This is not a sufficient way. Energy efficiency is a major factor in design wireless sensor networks. In existing system type1-Fuzzy logic is used for cluster head selection. Multi hop clustering is used here.

The existing algorithm is:

/∗ for each round∗/

1. Let N sensor nodes distributed randomly over M×M
2. region where k clusters are assumed
3. N sensor nodes are divided into different levels.
4. Level should be numbered according to the distance
5. from the base station.

6. Elect the CH at each level based on T2FL Model.
7. Apply Fuzzy if-then-else rule to elect the CH.
8. Select k-optimal CHs in each round
9. /∗for k-optimal CH ∗/
10. Transfer the data from one CH to other CH till it reaches at the base station but data should come from the upperlevel.
11. One sensor node with higher energy is elected as a
12. stand by (SB-CH) close to the base station to resume
13. the connectivity if any failure occurs at last CH (the
14. reason is that CH closer to BS consumes more energy)
15. /∗end of for ∗/
16. BS collects the aggregated data from last CH in the chain

/∗ End of rounds ∗/

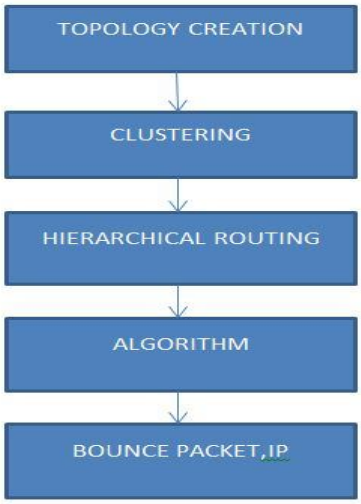

Figure 1: Existing Architecture

4. PROPOSED SYSTEM

In our proposed method as shown in figure 2, Topology of the network is formed here we use interval type2 fuzzy logic approach and clustering is done on the basis of multi hop clustering. Then packet monitoring is done and packets are received from system ports and classified it on the basis of checksum,flag,packetlength. Then the packets are classified into:

1) TCP packet
2) UDP packet
3) DNS

Then we have to check certain rules such that:

1) Whether the source IP and destination IP is equal
2) Whether the system receive packets from same port more than times

If any of the system violating these types of rules then there is some attacks is present. These rules are works like thread to more than system. So we can easily found more malicious systems.

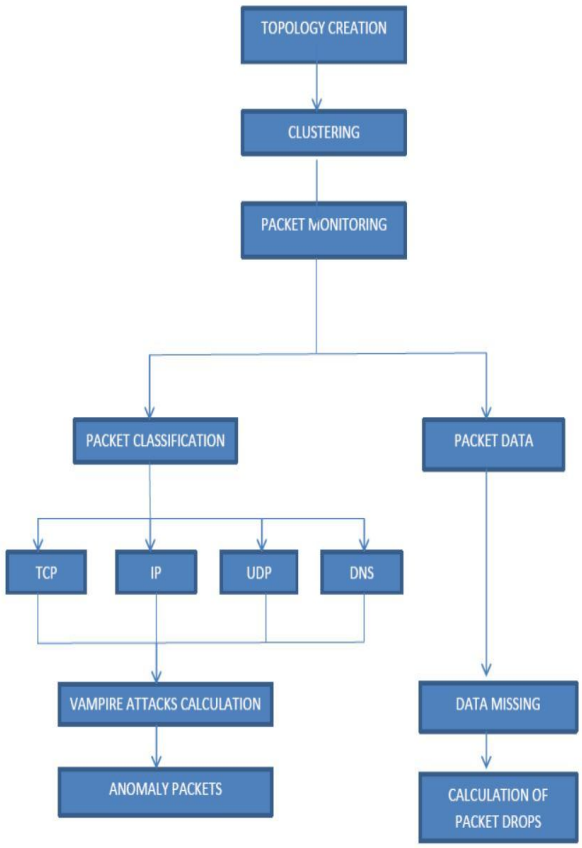

Figure 2: Architecture of proposed system : server

In this, the rules are travel as a thread to all other system in this network. So at a time more than one system can check that the presence of vampire attacks. Here the data and header of a packet were monitored. The malicious IP were found through the violation of certain rules. The vampire attack usage the packet flooding and RREQ flooding to establish the malicious connection during. Due to this target node flood the packets further and drain their energy and performance in network. Thus when the attack is

deployed than the first the number of broadcast in network is counted and a threshold value is determined. This technique is not algorithmic based it is rule based method. Whenever the rules are more efficient the method became more useful.

5. CONCLUSION

Wireless sensor network is a kind of ad-hoc network. Thereis a new kind of internal attacks called vampire attack drain the energy of each Sensor in the network, in this proposed work a vampire attack is investigated and an appropriate method is proposed for implementation for improving security and performance in network by identifying and removing suspicious node from the network. The developed technique is not algorithmic approach.

6. ACKNOWLEDGEMENT

We would like to thank, first and foremost, Almighty God, without his support this work would not have been possible. We would also like to thank all the faculty members of Mount Zion college of engineering, for their immense support.

REFERENCES

[1]V.Subha1, P.Selvi 2014, **Defending against vampire attacks in wireless sensor networks**, International Journal of Computer Science and Mobile Computing.
https://doi.org/10.1109/TNET.2004.833122
[2] .J.-H. Chang and L. Tassiulas**, "Maximum Lifetime Routing inWireless Sensor Networks,"** IEEE/ACM Trans.Networking, vol. 12,no. 4, pp. 609-619, Aug. 2004.
[3] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, **Secure sensor network routing: A clean-slate approach**, CoNEXT, 2006.
https://doi.org/10.1145/1368436.1368452
[4]Vincyumadevi**, INSENS: Intrusion-tolerant routing for wireless sensor networks**, Computer Communications 29 (2006), no. 2.
https://doi.org/10.1016/j.comcom.2005.05.018
[5]ImadAad, Jean-Pierre Hubaux, and Edward W. Knightly**, Denial of service resilience in ad hoc networks, MobiCom,** 2004.
https://doi.org/10.1145/1023720.1023741
[6] GergelyAcs, LeventeButtyan, and IstvanVajda, **Provably secure on demand source routing in mobile adhoc networks,** IEEE Transactions on Mobile Computing 05 (2006), no. 11.
https://doi.org/10.1109/TMC.2006.170
[7] Jae-Hwan Chang and LeandrosTassiulas**, Maximum lifetime routing in wireless sensor networks**, IEEE/ACM Transactions on Networking 12 (2004), no. 4.
https://doi.org/10.1109/TNET.2004.833122
[8] E Y Vasserman , N Hopper ,**Vampire Attacks: Draining life from wireless Ad hoc sensor networks**, IEEE Transactions on Mobile Computing,volume 12, issue 2 , published on feb 2013(pages 318-332)
https://doi.org/10.1109/TMC.2011.274