Minimize the Vampire Attack using WSN on Routing Protocol

Trupti Borgamwar
P.G Student Dept of Electronics Engineering Communication
TGPCET
NAGPUR,INDIA
truptiborgamwar@yahoo.co.in

Kanchan Dhote
Head of Dept. Electronics Engineering
TGPCET
NAGPUR, INDIA
kanchan.dhote@rediffmail.com

Abstract— In a wireless networks the future research direction in prevention of vampire attack by existing routing protocol. The objective of this project is to examine resource depletion attacks at the routing protocol layer, which attempts to permanently disable network nodes by quickly draining their battery power. In this project presents analysis of routing protocols namely AODV (Ad hoc on demand). These protocols are analyzed on five QOS (Quality of service) parameters: Throughput, Jitter, Delay, PDR (Packet delivery ratio) and Energy consumption. AODV is thus suitable for networks where nodes are having sufficient energy .The results are shown in this project after the analysis for five parameters using NS-2 software. To reduce vampire attacks clustering is used and the results are shown with the help of graphs.

Keywords- *Routing Protocols; AODV*

*****

I. INTRODUCTION

As WSNs become more crucial to the everyday functioning of human being and organizations, availability faults become less tolerable. Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance-vector, source routing, and geographic and beacon routing.[4]. A new routing path can already created path during expire time, it does not changing routing path because AODV routing protocol must maintain routing path during expire time. Therefore, we proposed improved AODV routing protocol for reset a new shortest routing path during sending a packet. AODV is a very popular routing protocol for sensor network. There are several implementations available. Routing information has a timeout associated with it as well as a sequence number. The use of sequence numbers allows to detect outdated data, so that only the most current, available routing information is used.[3]

Reactive routing protocols

These protocols are designed to minimize routing overhead. In place of tracking the changes in the network topology to continuously maintain shortest path routes to all destinations, these protocols determine routes only when necessary. The different types of On Demand driven protocols are Ad hoc On Demand Distance Vector (AODV), Dynamic Source routing protocol (DSR), Ad-hoc On-demand Multipath Distance Vector Routing (AOMDV) DSDV (Destination Sequenced Distance Vector).[7]

1. Ad Hoc on Demand Distance Vector (AODV)

The ad hoc on-demand distance-vector (AODV) routing protocol is an on-demand routing protocol; all routes are discovered only when needed, and are maintained only as long as they are being used. Routes are discovered through a route discovery cycle, whereby the network nodes are queried in search of a route to the destination node. AODV that allow it to discover and maintain loop free route.[3]

2. Ad-hoc On-demand Multipath Distance Vector Routing (AOMDV)

Ad-hoc On-demand Multipath Distance Vector Routing (AOMDV) Protocol is an extension to the AODV protocol for computing multiple loop-free and link disjoint paths. For each destination, a node maintains the advertised hop count, which is defined as the maximum hop count for all the paths, which is used for sending route advertisements of the destination.. Because the maximum hop count is used, the advertised hop count therefore does not change for the same sequence number.[7]

3. Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) is an on demand source routing protocol that employs route discovery and route maintenance procedures similar to AODV. If there is no valid route in the cache, the sender initiates a route discovery procedure by broadcasting a route request packet, which contains the address of the destination, the address of the source, and a unique request ID. As this request propagates through the network, each node inserts its own address into the request packet before rebroadcasting it. When a node receives a request packet and finds its own address recorded in the packet, it discards this packet and does not rebroadcast it further. Once a request packet arrives at the destination, it will have recorded the entire path from the source to the destination.[7]

4. Destination Sequenced Distance Vector (DSDV)

The discussed routing protocols are all reactive protocols in which the routes are established on demands. DSDV is a proactive routing protocol which maintains the route to the destination before it is required to be established. Nodes exchange their routing tables periodically or when it is required to be exchanged. Due to being aware of the neighbour's routing table, the shortest path towards the destination could be determined.[7]

II. LITRETURE SURVEY

Lina R Deshmukh and Amol D. Potgantwar "Prevention of vampire attacks in WSN using Routing Loop," Proceedings of IRF International Conference, 5th & 6th February 2014, Pune India.

Here explaining the sensing and pervasive computing ad-hoc low-power wireless networks are an exciting research. Prior security work has first focused on denial of communication at the routing or levels of media access control. In this paper find that all examined protocols are affected to Vampire attacks ,which are destructing, hard to detect, and are

 ISSN: 2321-8169
3635 - 3638

easy to carry out using as few as one malicious insider sending only protocol compliant messages. In case of worst case, a single Vampire can increase network-wide energy usage by a factor of O (N), where N in the number of nodes of network.[1]

Gowthami. M, and Jessy Nirmal "Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks" International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

In this paper mentioned that the Ad-hoc sensor network and routing data in them is a most significant research area. There are lots of protocols established to protect from DOS attack, but it is not perfectly possible. This project illustrates a technique to tolerate the attack by employing the Cluster Head. In case of each Vampire attack, the Cluster Head employs in this situation and distributes the packet to destination without dropping the packet. Thus give a successful and reliable message delivery even in case of Vampire attack.[2]

Elizabeth M. Royer "An Implementation Study of the AODV Routing Protocol"

In the paper mentioned that the Ad hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad hoc mobile networks. Because of the difficulty of testing an ad hoc routing protocol in a real-world environment. This paper details many of the changes that were necessary during the development of the implementation. Because protocol design is not yet an exact science, designers should take advantage of those tools which may aid them in validating the operation of their protocols. In the course of writing the implementation, some key changes needed to be made to both the protocol and the Linux kernel to enable AODV to operate correctly. As AODV continues to be refined, it is possible that further changes will be required, particularly when QOS operation is implemented. Additionally, tunnel management may also indicate the need for further modifications.[3]

III. RELETED WORK

Introduction

Clustering is a technique which selects the number of cluster head depends upon cluster nodes energy and the same is used to transfer the data. The proposed model is on Ad hoc on demand Distance Vector routing protocol and also compared with Encryption and Cryptography in terms of the parameters such as Throughput, Packet Delivery Ratio and Packet Delay Time.[6]

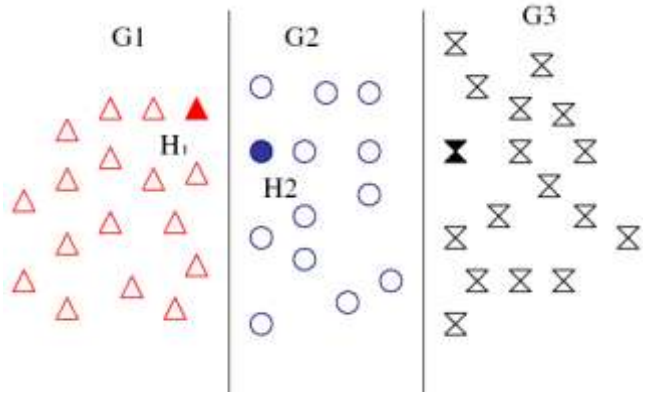

Figure 3.1 Multiple Cluster-head in small region.

- The communication in Cluster formation using cluster head and any node present on that cluster.
- First by the energy distribution select the cluster head for respective cluster and then communicate with other with the help of node.
- Node can send the data to the cluster head of the first cluster and then this data can send to the another cluster node and then to again cluster head. Using this procedure of data communication can increase the power consumption.

AODV (Ad-hoc On-demand Distance Vector)

AODV is a very popular routing protocol for sensor network. AODV has been standardized in the IETF as experimental RFC 3561. There are several

implementations available, for instance AODV uses a simple request-reply mechanism for the discovery of routes It can use hello messages for connectivity information and signals link breaks on active routes with error messages. Routing information has a timeout associated with it as well as a sequence number. The use of sequence numbers allows to detect outdated data, so that only the most current, available routing information is used. This ensures freedom of routing loops and avoids problems known from classical distance vector protocols.

IV. RESULTS

Introduction

Design Wireless Network

In this module we are designing the wireless Network with 30 nodes. And these are communicating with each other without any proper communication path so it required more energy to transmit the data from source to destination.

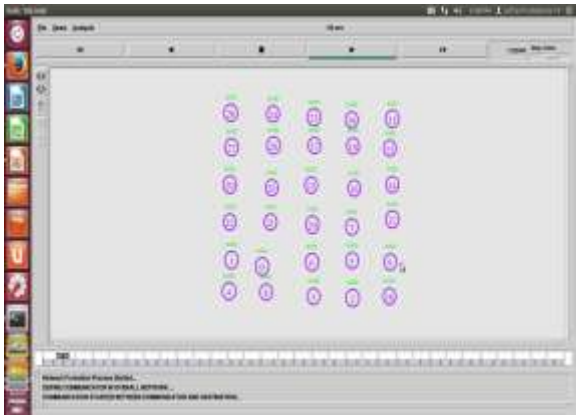

Figure 4.1 Design Wireless Network

The above figure shows that we here designing the wireless Network with 30 nodes. And these are communicating with each other without any proper communication path so it required more energy to transmit the data from source to destination.

 ISSN: 2321-8169
3635 - 3638

Comparative Graph of Quality of Service Parameters after applying Clustering, Compression & Encryption:

Delay: The average time taken by a data packet to arrive in the destination.
Delay= ∑ (arrive time – send time) / ∑ Number of connections
The lower value of end to end delay means the better performance of the protocol.

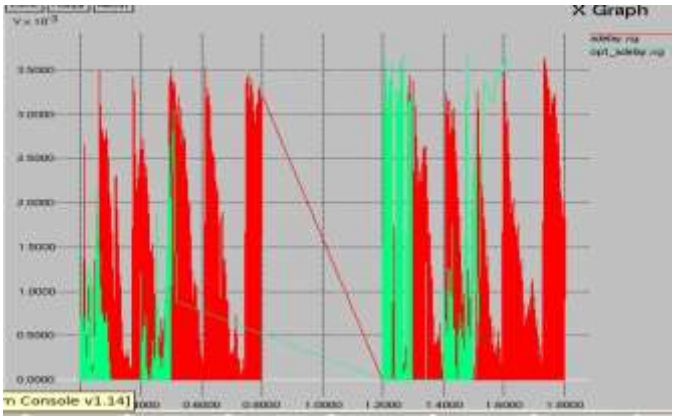

Figure 4.2 Comparative graph for delay

The above graph shows comparison of Delay. Here red colour indicates before clustering and , green colour indicates after clustering+ encryption+ compression is used. Graph indicates time(ms) on the x-axis and delay on y-axis.

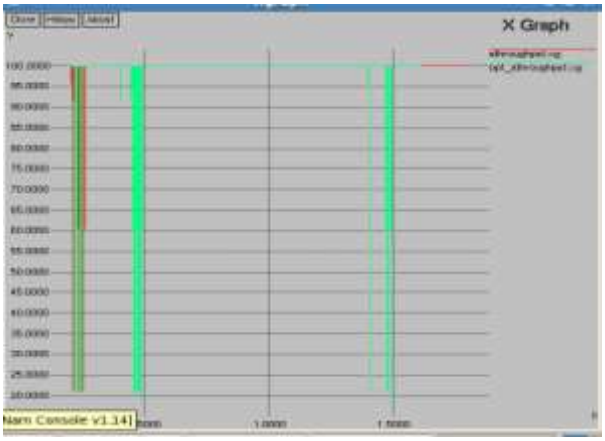

Figure 4.3 Comparative graph for Throughput

The above graph shows comparison of Throughput. Here red colour indicates before clustering and , green colour indicates after clustering+ encryption+ compression is used. Graph indicates time(ms) on the x-axis and throughput on y-axis.

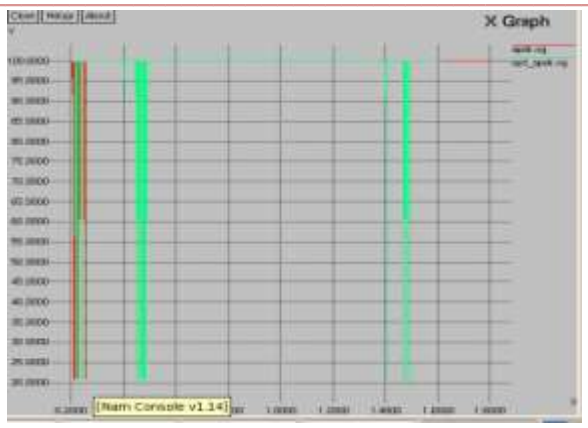

Figure 8.3 Comparative graph for Packet Delivery Ratio (PDR)

The above graph shows comparison of PDR(packet delivery ratio). Here red colour indicates before clustering and , green colour indicates after clustering+ encryption+ compression is used. Graph indicates time(ms) on the x-axis and PDR(packet delivery ratio) on y-axis.

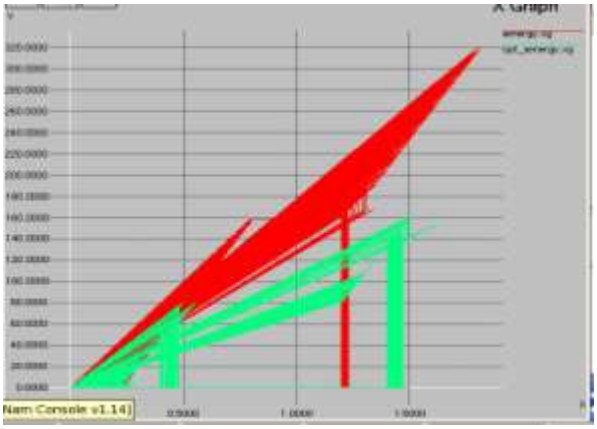

Figure 8.4 Comparative graph for Energy Consumption

The above graph shows comparison of energy consumption. Here red colour indicates before clustering and , green colour indicates after clustering+ encryption+ compression is used. Graph indicates time (in ms) on the x-axis and energy consumption (in joules) on y-axis.

 ISSN: 2321-8169
3635 - 3638

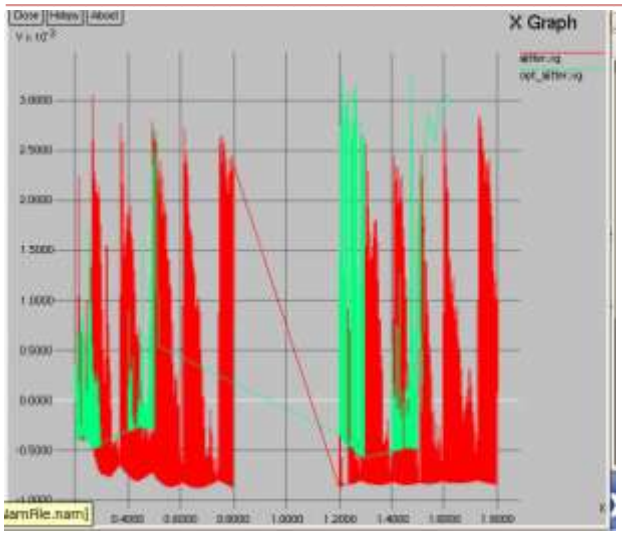

Figure 8.5 Comparative graph for Jitter

The above graph shows comparison of jitter. Here red colour indicates before clustering and , green colour indicates after clustering+ encryption+ compression is used. Graph indicates time (in ms) on the x-axis and jitter (in joules) on y-axis.

V. CONCLUSION

In this paper, we have presented the application of Clustering, with he AODV protocols have been implemented in NS-2 and are analyzed on the basis of five crucial parameters: Throughput, delay, jitter , PDR and energy consumption. After applying the clustering on the Quality of service parameters are improved. Simulation results showed that the performance of Cluster formation scheme is better for efficient data transmission from sender to receiver by updating the new shortest path and also resolving link break between source and destination.

ACKNOLEDGEMENT

We would like to thank Eugene Y.Vasserman, M ,G. Vijayanand, K.Vanitha, Vidya M, SHARNEE KAUL and our anonymous reviewers for their very helpful comments on earlier drafts of this paper.

REFERENCES

[1] LinaR.Deshmukh and Amol D. Potgantwar“ Prevention of vampire attacks in WSN using Routing Loop,” proceedings of IRF International conference,5th& 6th Feb 2014,Pune India

[2] Gowthami.M, and Jessy Nirmal.A.G “Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks”, IJARCST Vol. 2. Jan-Mar 2014

[3] Elizabeth M. Royer “An Implementation Study of the AODV Routing Protocol”

[4] Eugene Y. Vasserman and Nicholas Hopper “Vampire attacks: draning life from wireless ad-hoc sensor networks”, IEEE TRANSACTIONS ON MOBILE COMPUTING VOL.12 NO.2 YEAR 2013

[5] S.Blessy Vedha, “ A Captivating Approach for Disclosing Vampire Intrusion in WSN” *2014, ICCTR*

[6] Ramesh and Dr. K.Somasundaram “A Comparative Study of Clusterhead Selection Algorithms in Wireless Sensor Networks”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011

[7] Yu-Doo Kim, Il-Young Moon, Sung-Joon Cho “A Comparison of Improved Aodv Routing Protocol Based on Ieee 802.11 and Ieee 802.15.4”, Journal of Engineering Science and Technology Vol. 4, No. 2 (2009)

[8] Susan Sharon George and Suma R “ Attack-Resistant Routing for Wireless Ad Hoc Networks,” International Journal of CS & IT, vol.5.(3),2014.