International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 32451-32458
© Research India Publications
http://www.ripublication.com

Prevention & Detection of Intrusion & Increase in Lifetime of Ant-Networks using OLSR

j. Jijin Godwin[1] and S. A. Dhivyamalini[2]

[1]Assistant Professor,
Velammal Institute of Technology, Panchetti-601204, TN, India
[2]Course of Embedded System Technologies,
Velammal Institute of Technology, Panchetti-601204, TN, India
[1]jj03ece@yahoo.com, [2]dhivscool19@gmaii.com

Abstract

In WSN, each and every node will consume powerfrombattery resourcesfor packet transmission. Apart from battery power consumption, security threatening is also a key issue in wireless sensor networks. The malicious node might hack information from any network and leak its packets to some other network, cause security problems. In the existing system the wireless networksareas follows, considering the wireless routing in ad hoc networks, each node could act as router and hence all nodes in WSN would perform carry forward information. So the existing technique would add more points of vulnerability to the network. In this paper, we propose a novel method, to bringthe benefits of Optimized Link State Routing (OLSR) protocol and Ant network. Points of vulnerability are highly reduced due to the ant network and thisnetwork lifetime is enhanced thereby earlier die of node or specific path is avoided.

Keywords— adhoc network , olsr ,security, wsn, lifetime.

I. Introduction

In designing an Ad-hoc network, the fundamental challenges to be facing that are: maximizing network life time and securing data packets.As each sensor node equipped with limited battery power, it is mandatory to keep node in long living condition to from stable network. In the last few years, different methods were developed to overcome these challenges such as network protocols, data fusion algorithms using low power, energy efficient routing, and locating optimal sink position. Mobile nodes are powered by battery, effective utilization of battery energy is very important. The Battery life of individual node can also affect the overall network communication performance, when a node tire to its available energy, it ceases to function and the lack of mobile hosts can result in network partitioning. These reasons will cause the reduction of power consumption is an important issue in ad hoc wireless networks. Earlier routing protocols tend to use shortest path algorithms (minimum hop count) without any consideration of energy consumption, often resulting in rapid energy exhaustion for the small subset of nodes in the network which experiences heavy traffic loads. In recent years a number of poweraware metrics have been proposed in [1]-[4]. The majority of these metrics has been applied to on demand routing protocols like DSR.Proactive routing protocols, also known as table driven, are modifications of traditional prior routing table and distance-vector based routing protocols for wired networks. Every node in network exchange periodic information regards each of its neighboring node's status. This is in the aim of making routing tables up to date all the time. Furthermore, routes are maintained for all reachable destinations. Hence, routing could start immediately whenever data traffic is present.

The concept of Multi-Point Relays (MPRs) introduced in the OLSR protocol [3]. The key idea is to limited number of retransmissions required for a node to flood a packet in the entire network. For this purpose, each node selects a subset of its one-hop neighbors to be responsible of forwarding its broadcasted packets. Those nodes are called MPRs. Certainly these feature contributes to minimization of the overall network energy consumption. However, as a non-uniform routing protocol,In periodic message exchanges itself every node came to know about their neighbor MPR nodes, if the structure of the network changes or the MPR node goes out of network, another neighboring nodes will be chosen as MPR and all other nodes were informed about the change in MPR nodes. In fact, energy is drained more quickly in MPRs nodes than in no-MPRs ones. Therefore, this paper proposes to transmit data packets as followed in ant network. Particularly, maximum lifetime routing approach that avoids nodes with poor energy profiles should be adopted.

II. RELATED WORKS

The routing protocols for mobile networks can be classified into four broad categories: proactive, reactive, hybrid, and cluster-based. These protocols try to satisfy various properties to reach the best compromise in term of scalability, mobility support, and energy consumption. The want to overcome the energy efficiency problem concerning with the constraints imposed by battery capacity and heat dissipation which are opposed by the desire of miniaturization and portability. Energy efficiency is a critical design consideration in battery powered and densely deployed wireless sensor networks, which can be achieved by minimizing the number of messages transmitted all along the data collection process. Accompanying the works include clustering, network coding, in-network data aggregation, and approximate data collection. In recent years a number of power-aware metrics have been proposed at the network. Here we present a brief description of the most relevant power-aware routing metrics proposed recently.

MEL AODV

The utmost Energy Level of Ad Hoc Distance Vector (MELAODV) is based on alternate maximum remaining energy routes in each node to optimize the network lifetime and to accomplish efficient utilization of node energy. This algorithm selects the minimum cost and highest energy path. The path discovery process is initiated at any time a source code requires to communicate with another node for which it has no routing information in its table. Each node persevere two segregate counters: a node sequence number and a broadcast id. If the destination or the intermediate node moves away (or the local energy of any of them is not enough), a route maintenance process is initialized and performed by sending a link failure notification message to each of its upstream neighbors to ensure the deletion of that particular part of the route. Once the link failure notification message reaches source node, it restarts a new route discovery process.

Energy Aware DSR

E-DSR is designed to use the paramount energy route to transmit data packets. When a node desired to send data packets to some destination node, it first broadcasts a route request packet to its neighbors. Every energy efficient neighboring node not beyond a broadcast range adds their node id to the route request packet, updates the total energy field in the route request packet using their local energy and then rebroadcasts. To maximize the lifetime of nodes, only energy-efficient ones participate in this route discovery process. Eventually, one of the broadcast messages will reach a destination or a node with a recent route to the destination. In original DSR, each node maintains a route cache; it first checks its own cache for a route that matches the requested destination. Maintaining a route cache in every node reduces the overhead generated by a route discovery phase. It noted that e-DSR has multiple routes available in its route cache while e-AODV has a single route in its route table.

A. EESDA

In Energy-efficient, secure, highly accurate, and scalable scheme for data aggregation (EESSDA) achieved by establishing secure channel and slicing technology. The EESSDA scheme don't need encryption and decryption operations concurrently at the data aggregation, which saves energy and obtain huge accuracy of aggregation results. Meanwhile, in EESSDA scheme, the advanced deployment of shared information between nodes is not required, making the networks with good scalability.

However , many ad-hoc energy aware protocols concentrates on transmitting the entire packets through predicted low energy path , upon one path failure or over drain , it recommends to alter or reroute the packets travelling path. In this paper, we propose to split the packets to multiple numbers in the source itself. It provides more security than existing methods. A case said the entire data broken and 100 new sub packs takes different path. When the intruder tries to hack information, fortunately it takes attempt on hacking a very small quantity of data, from which the entire message would not be snooped. In addition to that, we propose a node behavior analysis to find the anomaly nodes.

III. METHODOLOGY

A.MultiPoint Relay

In WSN, normally source floods its packets to all neighbor nodes. The receiving node could take the decision on forwarding packets to its neighbors, this process continues till the specified packet reaches its destiny. In olsr protocols, all the nodes would not participate in the transmission. For a group of nodes there some nodes act as Multi Point Relay nodes. Transmission of packets carried and forward process to be held by only these MPR nodes.

Source in this network does not forward its packets to all of its neighbors, instead, it source forwards its packets only to MPR nodes. In this case any hackers would hack data only from these MPR nodes. Because intruder cannot hack data from the nodes, those are not participating in the transmission. Hereby the points of vulnerability highly reduced in proposed methods. The reduction in unwanted flooding of packets further reduces the traffic in network and hence increases life time.

B. Prolonging Network Life Time

In normal packet transmission, the data travels only through specific path. In that case the nodes on particular path drain out earlier from other nodes. Due to that earlier drain out the set of nodes might be isolated from communication and it could not be communicated further. Moreover, the low power nodes might not be able to transmit its own data to its destiny. The link failure occurs along one certain path fall down or will be failed soon. This paper proposes merging of olsr protocol in Ant network. Ant is a wireless Multicast wireless sensor networks technology uses 2.4Ghz ISM band. Ant is a multi-message transmitting techniques uses the full data bandwidth. The nodes in ant network deployed to share small amount of data in wireless sensor applications and hence consumes less power. Before forwarding the packets, each node in the network splits the packet and diverts it in two separate directions. Initially the source node splits its packets and forwards it to set of MPR nodes. These MPR nodes further break the packets and send it to its neighbor MPR available in the direction of destiny node. These process carried by all intermediate participating MPRs till reaches sink. The sink node aggregates the data from various path and reassemble it to recover original data.

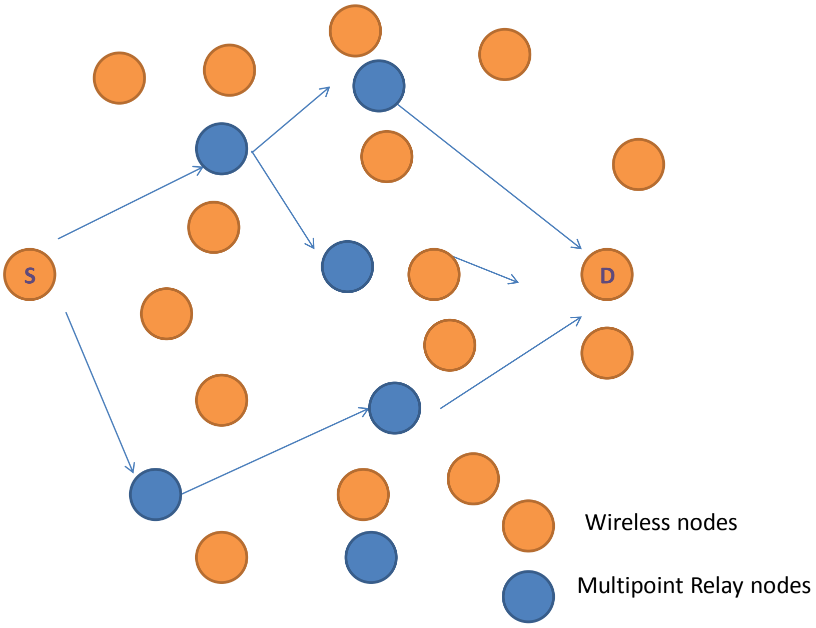

Fig 1.1 OLSR based Ant network path selection

By this approach the entire traffic is shared and carried out by deployed nodes. This factor causes the uniform drying in all participated nodes. Here the problem of more drain out from set of nodes eliminated and more deployed nodes contribute low power to the communication. The node, which is apart from network, would be intruder or the existing participating node, itself become malicious node. The former case can be predicted easily and later one is not easy. The behavior of anomaly node differs from other normally behaving nodes. This paper proposes a node behavioral analysis it detects the misbehaving nodes. Upon detection this method isolates the node from multi point relay node selection.

C. Parameter Analysis

The misbehaving node definitely varies in its behavior from other nodes. The changes in behavior of malicious node were measured by its parameter variation. This paper measures the parameter such as time delay introduced by nodes, energy consumption of nodes, Jitter packet loss and packet delivery ratio.

The intruder node introduces the additional time delay to the network. The time delay required by a normal node to receive and forward, is lesser than the malicious node, which is trying to modify or reroutes packets to wrong destiny. Whenever the node alters its behavior, it tries to flood excess or duplicate packets and redundant packets in the network. These redundant packets cause the extra time delay to the original data.

The malicious nodes consumes more energy, it spends more battery power for packet transmission. It happens, due to the excess packets or the no of packets variation in inlet and outlet transmission. When the packet not reaches its destiny the respective acknowledgement not received by the source. The packet delivery ratio will gradually decrease if intruder hacks packets.

IV. Results and Discussion

The Fig 1.1 shows the time delay variation introduced by normal nodes is linearly increasing and after certain time, it remains constant. But in malicious case the delay introduced between successive packets is gradually increased.

The Fig 1.2 describes the case at which the normally behaving nodes defects the transmission by becoming malicious. This case is difficult to find. As readings taken and plotted in graph shows the energy drain out by normal and abnormal nodes.

It clearly indicates the battery consumption of both the nodes looking similar till it reaches the point of change at which the normal behaves abnormal. After the point of change the energy spent by two such nodes highly varies.

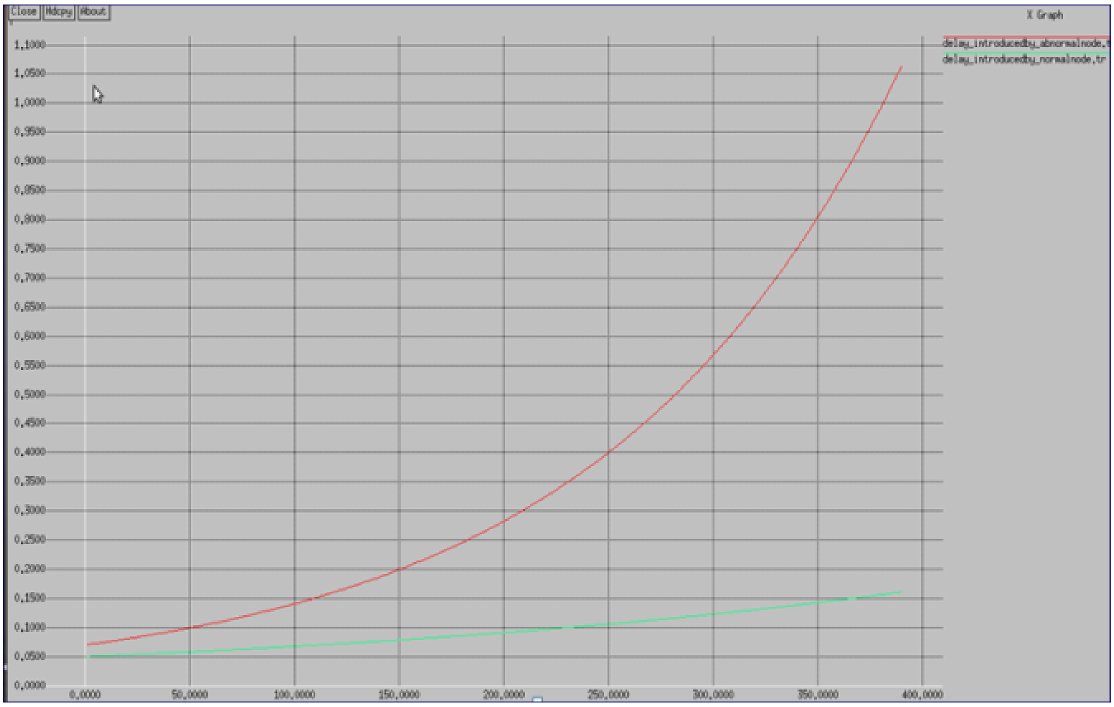

Fig 1.2 Time delay vs no of packets

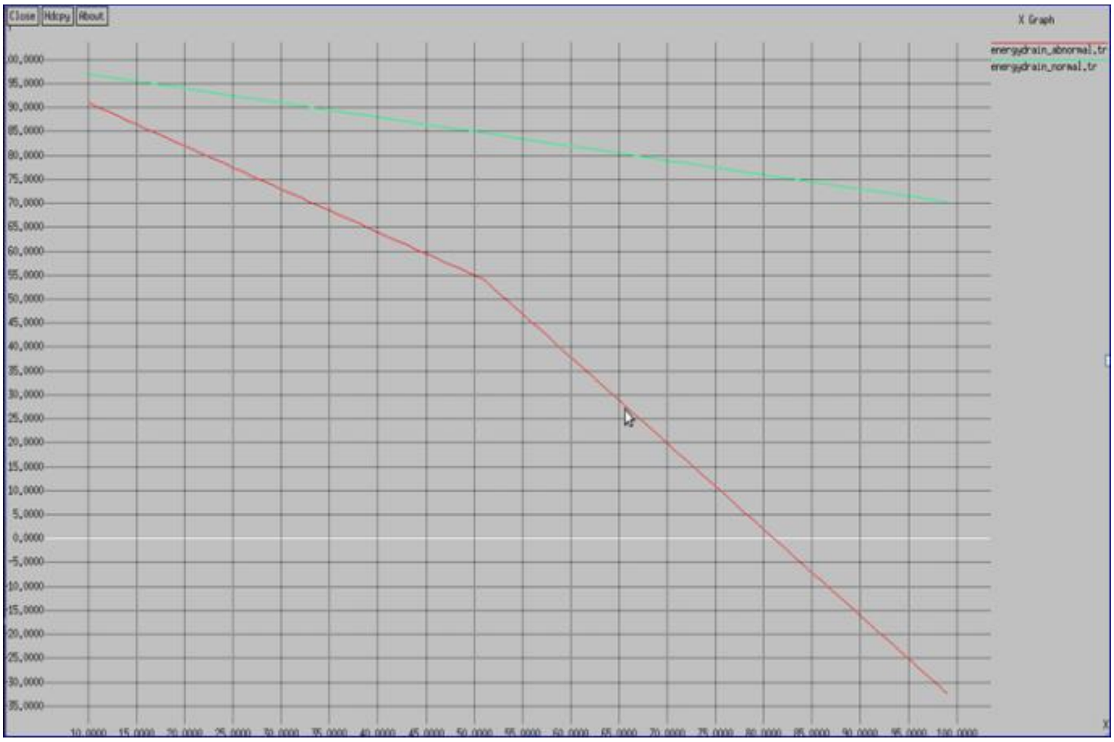

Fig 1.3 Energy drain vs packets

The packet lost occurred by normal nodes would be considerably reduced, unless the destination is not reachable for its attempt. Sometimes the no of inlet and outlet packets highly varies in case the intermediate node is a malicious node. In such cases the packet delivery ratio decreases with no of packets passes through it increases.

V. CONCLUSION

This paper proposed a method to implement Ant network in olsr based protocol and utilized the beneficiary of both methods. Through the various simulation results the proposed method has found as more effective in energy saving scheme and provide more barrier to vulnerability of security in ad-hoc networks. This method allows more no of MPR nodes to contribute their small amount of energy to the communication and hence the lifetime of network considerably increased.

VI. REFERENCES

[1] D. Kim, J.J. Garcia-Luna-Aceves, K. Obraczka, J. Cano, and P. Manzoni. “Power-Aware Routing Based on TheEnergyDrain Rate for Mobile Ad Hoc

Networks” IEEE International Conference on Computer Communication and Networks, October 2002.

[2] J.-E. Garcia, A. Kallel, K. Kyamakya, "A Novel DSR-Networks," in 58th IEEE Vehicular Technology Conference (VTC Fall. 2003), 6-9 Oct. 2003, pp.: 2849 – 2854.

[3] C.Taddia, A.Giovanardi, G.Mazzini, M.Zorzi, “Energy efficient unicast routing protocols over802.11b,” in IEEE Global Telecommunications Conference, (GLOBECOM’05), 28 Nov.-2 Dec. 2005.

[4] A.McCabe, A.Cullen, M.Fredin, L.Axelsson, “A power consumption study of DSR and OLSR,” in IEEE Military Communications Conference (MILCOM’05), 17-20 Oct. 2005, pp.1954 – 1960.

[5] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum and L. Viennot, "Optimized link state routing protocol for ad hoc networks", in IEEE INMIC, 2001.

[6] “AODV and DSR energy-aware routing algorithms: a comparative study”,Heba Abu-Matter, Maha Al-HunatiIJCSIInternational Journal of Computer Science Issues, Vol. 9, Issue 6, No 1, November 2012.

[7] J.H.Chang and L.Tassiulas,”Energy conserving routing in wireless routing in wireless adhocnetworks”,inproc.IEEE INFOCOM,2000,vol.1,pp.22-31.

[8] Chauhan, R.K.Chopra, “Energy efficient routing in mobile adhoc network with capacity maximization”,IJCASpec.Issue Mob. Ad-hoc Netw,2010.

[9] B.Kannhavong,H.Nakayama,andA.Jamalipour, “A survey of routing attacks in mobile adhocnetworks,”IEEEtrans.wireless Commun.,vol.14,no.5,pp 85-91,oct.2007.

[10] T.Clausen and U.Herberg, “security issues in the optimized link state routing protocol version 2(olsr v2)”,Int.J.Netw.security Appl.,2010.