ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 11, May 2016

International Conference on Innovations in Engineering and Technology (ICIET'16)

6th & 7th April 2016

Organized by

K.L.N. College of Engineering and Technology, Madurai, Tamil Nadu, India

E.S Tar Alert Protocol for Wireless Sensor Network

Pitchai Murugan G[1], Sanjeeve Kumar S[2]

PG Scholar, Dept. of CSE, Anna University Regional Campus, Keelakuilkudi, Madurai, India[1]

Assistant Professor, Dept. of CSE, Anna University Regional Campus, Keelakuilkudi, Madurai, India[2]

ABSTRACT: In multihop wireless networks, when a mobile node needs to communicate with a remote destination, it relies on the other nodes to relay the packets. We also consider heterogeneous multihop wireless networks (HMWNs), where the nodes' mobility level and hardware/energy resources may vary greatly. E-STAR for establishing stable and reliable routes in heterogeneous multihop wireless networks. It combines payment and trust systems with a trust-based and energy-aware routing protocol. The payment system rewards the nodes that relay others' packets and charges those that send packets. The trust system evaluates the nodes' competence and reliability in relaying packets in terms of multi- dimensional trust values. . In this paper, additionally we propose a alert protocol will satisfy network user requirements in terms of energy and security to improve reliability. Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. To offer high anonymity protection at a low cost, we propose an Anonymous Location-based Efficient Routing proTocol (ALERT). ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. The attacker node will drop the packets also route break happens to overcomes this problem alert protocol is used. Simulation results demonstrate in NS2 that our routing protocols can improve the packet delivery ratio and low energy consumption.

KEYWORDS: packet dropping and selfishness attacks, trust systems, and secure routing protocols, anonymity, Routing protocol**.**

I. INTRODUCTION

The interest in multihop wireless networks such as mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), multihop cellular networks (MCNs), and wireless mesh network (WMN) has been increasing significantly [1], [2], [3], [4]. In these networks, a node's traffic is usually relayed through other nodes to the destination. Multihop packet relay can enable new applications and enhance the network performance and deployment. It can extend the communication range using limited transmit power, improve area spectral efficiency, and enhance the network throughput and capacity [5], [6]. Moreover, multihop wireless networks can be deployed more readily and at low cost in developing and rural areas. However, due to involving autonomous and self-interested devices in packet relay, the routing process suffers from new security challenges that endanger the practical implementation of these networks. We also consider heterogeneous multihop wireless networks (HMWNs), where the nodes' mobility level and hardware/energy resources may vary greatly. HMWNs can implement many useful applications such as data sharing and multimedia data transmission . Cooperation stimulation mechanisms [7], [8] use credits (or micropayment) to motivate the rational packet droppers to relay packets. The nodes earn credits for relaying the others' packets and spend them to relay their packets; The nodes earn credits for relaying the others' packets and spend them to relay their packets,

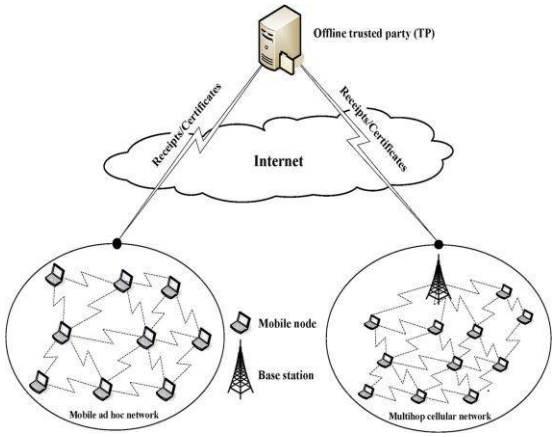

Fig. 1. Architecture of MWNs.

i.e., these mechanisms make relaying packets more beneficial for the nodes than dropping them. However, cooperation stimulation mechanisms cannot identify the irrational packet droppers assuming that the nodes will relay the packets faithfully using credits. This assumption cannot be guaranteed in MWNs because, unlike single-hop networks that are run by the equipment of the operators, packet relay is performed by user-provided equipment. Some attackers may drop packets to disrupt the packet transmission process, and broken nodes may have a software or hardware fault that prevents them from relaying the packets successfully. In Internet Protocol networks, the malfunction of the network equipment is an important source for network unavailability [9]. It is impossible to know whether a packet is dropped for malicious or no malicious reasons, e.g., due to faulty nodes and bad channel condition; therefore, it is necessary to measure the nodes' frequency of dropping packets, and the nodes that consistently drop the packets are considered attackers because they pose a severe threat to the proper operation of the network [7], [8].

Now a day's using mobile Ad-hoc Network, numerous wireless applications can be developed and these are used in much number of areas like mainly in military, education, commerce, entertainment. MANET- MANET's basic features are self organizing and independent infrastructure. All the nodes in the network are mobile and use wireless communications to communicate with other nodes. But as perspective of security of MANET, these networks get easily broken their security. Mainly data get lost or stolen by tampering and analyzing data and traffic analysis eavesdropping method or attacking routing protocol. For this security issue one solution is to use anonymous routing in the network that cannot be identified by any other nodes or attacker or observer. Although this anonymous routing is not required in general application .but it is very essentitial in Military, Banking like application, where security of communication is main purpose. Anonymous routing provides secure communication between two nodes by hiding nodes original identity and prevents these nodes from traffic analysis attacks of adversaries.

II. RELATED WORK

A.Secure and Reliable Routing Protocols for Heterogeneous Multihop Wireless Networks

Mohamed M.E.A. Mahmud, Xuedong Lin AND Xiamen (Sherman) Sheen propose E-STAR for establishing stable and reliable routes in heterogeneous multihop wireless networks. E-STAR combines payment and trust systems with a trust-based and energy-aware routing protocol. The payment system rewards the nodes that relay others' packets and charges those that send packets. The trust system evaluates the nodes' competence and reliability in relaying packets in terms of multi-dimensional trust values. The trust values are attached to the nodes' public-key certificates to be used in making routing decisions. We develop two routing protocols to direct traffic through those highly-trusted nodes having sufficient energy to minimize the probability of breaking the route. By this way, E STAR can stimulate the nodes not only to relay packets, but also to maintain route stability and report correct battery energy capability. This is because any loss of trust will result in loss of future earnings. Moreover, for the efficient implementation of the trust system, the trust values are computed by processing the payment receipts. Analytical results demonstrate that E- STAR can secure the payment and trust calculation without false accusations.

The notion of trust used in this paper is defined as the degree of belief, the expectation, or the probability that a node will act in a certain way in the future based on the nodes past behavior. Trust values are calculated from the past behavior to predict the expected future behavior. For instance, people will not assign critical jobs to someone with a record of failure since there is a good reason to believe that he will not get the job done properly. Similarly, if a node has broken a large percentage of routes in the past, there is a strong belief that this node will break routes with high probability in the future, and thus the routing protocol should avoid it. The trust values are computed to depict the nodes' reliability and competence in relaying packets.

To secure the routing protocol, E-STAR can satisfy the following requirements: 1) valid routing packets (RREQ and RREP) cannot be fabricated; 2) invalid routing packets cannot be propagated in the network; 3) valid routing packets cannot be altered in transit without detection, except according to the normal functionality of the protocol; 4) routing loops cannot be formed by malicious action; 5) stale routing packets are not accepted by the nodes or propagated in the network; and 6) unauthorized nodes' packets are not accepted by the authorized nodes.
We have proposed E-STAR that uses payment/trust systems with trust-based and energy-aware routing protocol to establish stable/reliable routes in HMWNs. E STAR stimulates the nodes not only to relay others' packets but also to maintain the route stability. It also punishes the nodes that report incorrect energy capability by decreasing their chance to be selected by the routing protocol. We have proposed SRR and BAR routing protocols and evaluated them in termsof overhead and route stability. Our protocols can make informed routing decisions by considering multiple factors, including the route length, the route reliability based on the nodes' past behavior, and the route lifetime based on the nodes' energy capability. SRR establishes routes that can meet source nodes' trust/energy requirements. It is useful in establishing routes that avoid the low-trust nodes, e.g., malicious nodes, with low overhead. For BAR, destination nodes establish the most reliable routes but with more overhead comparing to SRR.

III. PROPOSED SYSTEM

In this proposed system we propose the ALERT protocol with E-STAR to improve the security in the region. E-STAR provides the method to select the intermediate relay nodes based on the payment and trust system. Additionally to this we add ALERT protocol to enhance the route stability and the security in the region. Generally an attacker either attacks the routing path or the node. Therefore to avoid this, we proposed the E-STAR with ALERT.

A. Alert-Anonymous Location Based Efficient Routing Protocol

ALERT can be used in different network models with node movement patterns. Such as random way point model and group mobility model. Using network model information attacker may find out location of nodes. So anonymity may get threaten. Therefore, an anonymous communication protocol is needed which can provide untraceability to strictly ensure the anonymity of sender. As well as attacker try to block the data packets by injecting packets on a routing path. Therefore, route should also be undetectable. And with help of intersection attack on traffic destination node can be detected, so destination node also needs the protection anonymity. Pseudonym and Location of Node defines dynamic pseudonym is another name or identity given to node. In ALERT pseudonym used as node identifier with replacement of its real MAC address. Nodes MAC addresses
can be used to trace nodes existence in the network. Therefore replacing MAC address with pseudonym is the main advantage of ALERT protocol. This pseudonym is the combination of MAC address and Current time stamp. But if this information is known by attacker then it is easily find out the node. Therefore, to prevent this time stamp can be randomly selected. This pseudonym is not permanent; it expires after a specific time period so that attacker cannot associate the pseudonym with nodes. With this pseudonym there is one problem is changing pseudonym frequently create routing uneasy. Therefore these pseudonym changes frequently should be appropriately determined.

B. The ALERT Routing

Generally ALERT provides unpredictable and dynamic routing path, which having no. of dynamically selected intermediate nodes.

1. First ALERT partitions given network area into two zones as horizontally (or vertically).
2. Then again split every partition into two zones as vertically (or horizontally). This process called as hierarchical zone partition.
3. After partitioning ALERT randomly select a node in each zone at each step as an intermediate relay node, in this way ALERT provide dynamically creating an unpredictable routing path.

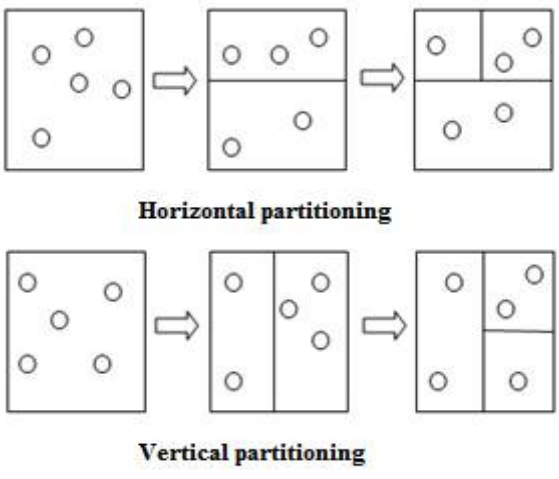

Fig 2. Partitioning methods

Above fig.2 shows both partitioning, here we generally network considered in rectangle form. In this rectangle circle consider as nodes. Consider one example of routing in ALERT. In this example we first horizontally partition network then vertically and so on. While this partitioning each data source of forwarder node checks whether itself and destination node is not in same zone. If it is not then partitioning continues. In above fig where the destination node locates that zone is called as destination zone denoted as ZD and that zone having k nodes, which is used to control the degree of anonymity.

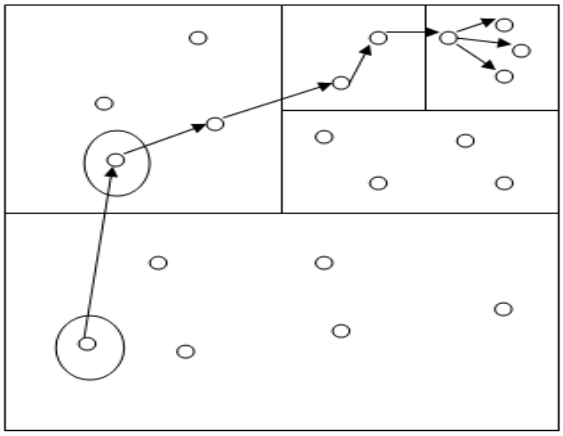

Fig 3. Zonal Routing of Nodes

While in routing first source node randomly chooses a node in other zone known as temporary destination (TD) and then uses GPSR routing algorithm to send the data to node close to TD. This process continues to reach data to destination node. A node closer to TD known as Random Forwarder (RF) .But in destination zone data is broadcasted in ZD to k nodes which provides k anonymity i.e. attacker or observer does not known at destination node.

C. Location of Destination Zone

Zone position is made from the upper left and bottom right coordinates of a zone. It is used by each packet forwarder to check whether it is separated from destination zone or not, to calculate zone position we have H denotes total no. of partitions in order to produce ZD and no. of nodes i.e. k and node density ρ

$H = \log2(\rho.G/k)$

Where as G=size of entire network area

Using H and G the position (0,0) & (Xg , Yg) of entire network area and position of destination node d the source can calculate the zone position of ZD.

D. Packet Format

For successful routing between source and destination some information is needed, which is embeds in the packet by source and each packet forwarder node. For ALERT following packet format is use.

RREQ/RREP/NAK		P_S	P_D	L_{z_S}	L_{z_D}	L_{RF}
h	H	K^S_{pub}	$(TTL)_{K^{Kf}_{pub}}$	$(Bitmap)_{K^D_{pub}}$		data (NULL in NAK)

Fig.4 ALERT Packet Format RREQ/RREP/NAK- use to acknowledge the loss of packet. Ps- Pseudonym of a source. Pd – pseudonym of a destination.

Lzs & Lzd – are the position of Hth partitioned source zone and destination zone.

h- number of divisions.

H – maximum number of division allowed.

IV. SIMULATION RESULTS

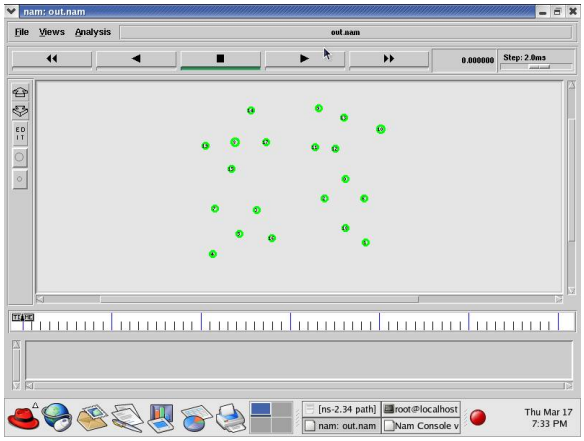

Fig.4 ALERT Initialization

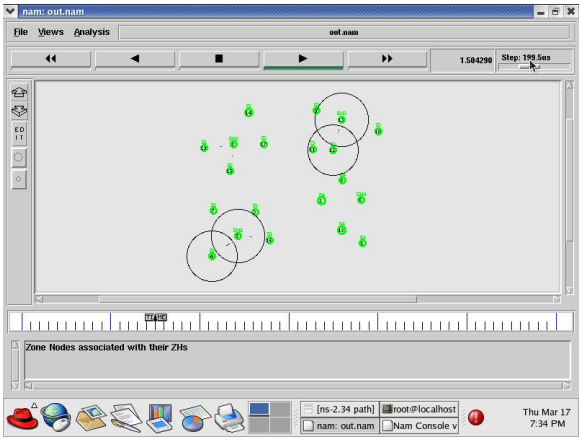

Fig 5. zone partitioning and data transferring

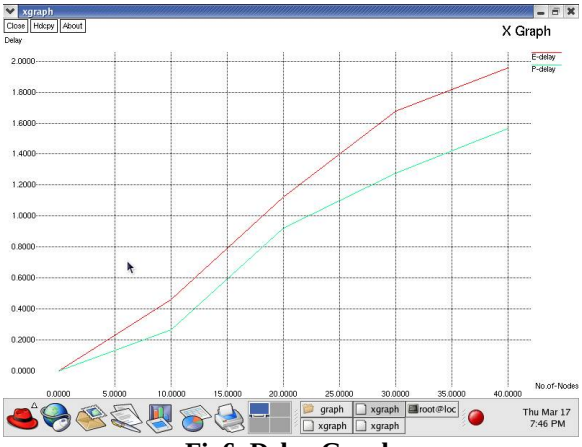

Fig6. Delay Graph

Fig 7. Throughput Graph

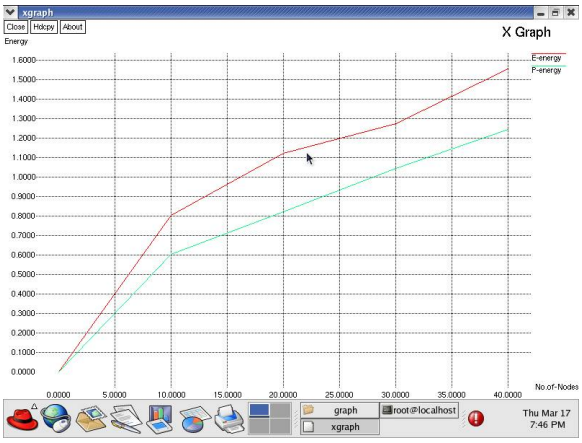

Fig 8. Energy Graph

V. CONCLUSION

E-STAR stimulates the nodes not only to relay others' packets but also to maintain the route stability. It also punishes the nodes that report incorrect energy capability by decreasing their chance to be selected by the routing protocol. The existing routing protocols, depend on either hop-by-hop encryption or redundant traffic which generate high cost. And some protocols are not providing complete source, destination, and route anonymity protection. ALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/ receivers.

REFERENCES

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi- Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.
[2] X. Li, B. Seet, and P. Chong, "Multihop Cellular Networks: Technology and Economics," Computer Networks, vol. 52, no. 9, pp. 1825-1837, June 2008.
[3] A. Abdrabou and W. Zhuang, "Statistical QoS Routing for IEEE 802.11 Multihop Ad Hoc Networks," IEEE Trans. Wireless Comm., vol. 8, no. 3, pp. 1542-1552, Mar. 2009.
[4] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A Robust Signature Scheme for Vehicular Networks Using Binary Authentication Tree," IEEE Trans. Wireless Comm., vol. 8, no. 4, pp. 1974-1983, Apr. 2009.
[5] P. Gupta and P. Kumar, "The Capacity of Wireless Networks," IEEE Trans. Information Theory, vol. 46, no. 2, pp. 388-404, Mar. 2000.
[6] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. IEEE/ACM MobiCom, pp. 255-265, Aug. 2000.
[7] J. Hu, "Cooperation in mobile ad hoc networks," Comput. Sci. Dept., Florida State Univ., Tallahassee, FL, Tech. Rep. (TR-050111), Jan. 2005.
[8] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation enforcement schemes for MANETs: A survey," J.Wirel. Commun. Mobile Comput., vol. 6, no. 3, pp. 319–332, May 2006.
[9] G. Iannaccone, C. Chuah, R. Mortier, S. Bhattacharyya, and C. Diot, "Analysis of link failures in an IP backbone," in Proc. IMW, Marseille, France, Nov. 2002, pp. 237–242. [10]M. Mahmoud and X. Shen, "ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks," IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997- 1010, July 2011.