ijournals International Journal of Software & Hardware Research in Engineering
ISSN No: 2347-4890 *Volume 2 Issue 4, April 2014*

HyPR : HYBRID PRIORITY BASED ROUTING

Ramya.S[1], Dr.Kalaikumaran.T[2], Dr. Karthik.S [3]

PG Scholar, Department of CSE, SNS College of Technology, Coimbatore-35[1].
Professor and Head , Department of CSE, SNS College of Technology, Coimbatore-35[2].
Professor and Dean, Department of CSE,SNS College of Technology,Coimbatore-35[3].

Abstract-The significant innovation of hardware manufacturing technology have boosted the implementation of Wireless Sensor Networks (WSNs).However WSN, have inadequate energy storage competence, it is essential to consider side by side security and energy efficiency in data gathering of WSN. Black-hole attack is one of the attack that interfere with information delivery. The Secure and Energy-efficient Disjoint Routing (SEDR) scheme is proposed to increase security and lifetime under both scenarios of single and multiple black holes. However SEDR scheme does not consider about the delay and packet loss. This paper enhances the existing scheme by using Hybrid priority based routing (HyPR) scheme which combines the structure of topology based routing with geographic routing. The HyPR scheme supports both unicast and multicast routing which guarantees secured packet transmission with minimum delay and packet loss.

Index Terms- Black hole; disjoint routing; network lifetime; security; topology routing ; geographic routing; delay .

INTRODUCTION

Wireless sensor network (WSNs) consists of hundreds or even thousands of nodes each with power unit, a sensing unit, a processing unit and communication capabilities to monitor the real-world environment. They are insignificant in size, and have wireless Communication competence within a short- range radio transceiver, a insignificant micro-controller, and a power supply. Wireless sensor networks (WSNs) are widely used in distinct fields. Most sensor network applications aim at monitoring or recognition of phenomena likes office building environment control, wildlife habitat monitoring, and forest fire recognition. Energy awareness is essential, especially in situations where it is not possible to exchange sensor node batteries so it is essential design issue in wireless sensor networks. Sensor networks are deployed in a hostile environment, security becomes extremely high - ranking as these networks are prone to distinct types of malicious outbreaks. Since the battery span margins the lifetime of a sensor node, power consumption is normally set as the first priority in developing security solutions.

There are different types of attack in WSNs but multipath routing is vulnerable to black hole attack. The black hole attacks or packet drop attack is a type of denial of service attack (DOS) in which router that is supposed to relay packets instead of discarding. The WSN are vulnerable to denial of service attack because of its low computation power, limited memory and computational power. The black hole refers to places in the network where incoming or outing traffic is discarded without informing the source that the data not reach the intended receiver. When examining the topology of the network the black holes themselves are invisible and can only be detected by monitoring the lost traffic. In black hole attack the opponent node may acquire routing algorithm and it can send same routes to the known source and hence endanger the information sent over the routes. In few cases the opponent may have mobility that increase the black holes which increase packet interception probability. The normal operation of the network may be affected by the DOS attack.

The black hole is one of the major attack which make security as a critical task. Designing routing mechanism that overcomes black hole attack is one of the effective methods for addressing security issues. In addition to security, in routing mechanism it is necessary to consider the end-to-end delay and packet loss. Without considering these to parameters the throughput of the network will be decreased because of collision in the network. Previous work mainly concentrate on delivering the packet in multiple disjoint path by maximizing both network security and lifetime by using disjoint multipath routing scheme with secret sharing. This analysis shows that network lifetime will not decrease if it is not less than four hops. The HyPR scheme significantly overtake existing routing strategies in terms of delay and packet loss in addition to network security and in different network situations.

RELATED WORK

To reduce end-to-end delay and packet loss in addition to security and lifetime of the network become a major issue. It is classified generally into two categories: 1) packet delivery, the packet is transmitted in variety of paths and 2) share delivery, i.e., transforming each packet into shares and then shares are forwarded along different path routes. Packet delivery mainly focuses on discovering node-disjoint or edge-disjoint paths for transmission; thus, it can enhance the security and robustness of networks. The Split Multiple Routing protocol was proposed to establish two maximally disjoint routes by flooding the ROUTE REQUEST (RREQ) message to the entire network. The security of sensor network routing protocols was analyzed , the multipath routing strategies are one of the effective countermeasure for the selective forwarding attack was determined. A Multidataflow Topologies (MDT) method was designed to bypass the selective forwarding attack by separating the sensor nodes into two- dataflow topologies. However, packet delivery duplicates the transmissions, which may lead to high energy consumption. Normally, share delivery uses secret sharing to enhance the security of packet transmission. Based on a secret-sharing algorithm, the intruders cannot decode the packet without intercepting a required number of shares. Therefore, the security performance of the network is improved. Moreover, as there is no need to duplicate packet transmissions, share delivery can significantly relieve the energy consumption of networks. The hybrid multipath scheme (H-SPREAD) was designed to improve both the security and reliability of WSNs which is based on a distributed N-to-1 multipath discovery protocol and secret sharing, a secure message transmission mechanism was proposed to continuously evaluate the performance of each route, and then, routing of subsequent shares is determined according to the rating of routes. Routing protocols for can be broadly classified into two categories. One category is topology-based and uses network topology data to connect different sensor nodes, and the other category of protocols called Geography-based routing protocols extends Global Positioning System (GPS) services to route the packets in sensor networks

Topology-based routing protocols were initially proposed have properties such as node mobility, distributed and self-organizing topology, non-existence of central control, etc,., the protocols are based on the IEEE 802.11 as a medium access control standard, and the trans- mission range is lower or equal to 250 m which is sufficient in such contexts where an important number of nodes tend to move with low speed. However, this transmission range is not enough for the transmissions between nodes because of their very high speed which made these transmissions instable. Consequently, topology-based routing protocols have been applied to WSNs but with the IEEE 802.11p standard which allows the transmission range to reach 300 m at least in order to make the network more stable Also, the routes used to disseminate data between nodes have a short time of life compared with routes used by others. This situation conducts to network partitioning .Consequently, discovering routes in this case of topology-based routing, the setup of topological end-to-end paths between a source and a destination before sending the packets is the fundamental step. These topology-based routing protocols can be reactive or proactive. The most common routing protocol that has been applied to WSNs is the Ad hoc On-demand Distance Vector (AODV) protocol. The route discovery method of AODV is based on routing tables which store the routes toward multiple destinations. Each destination is indicated using only the next hop node to reach this destination. The source disseminates a Route REQuest (RREQ) to its neighbours which in turn sends the same packet to their neighbours and so on, until the final destination is reached. Once the route request reaches the destination or an intermediate node which knows the path toward the destination, a Route REPlay (RREP) is sent back to the source node through the reverse route. AODV uses a sequence number to discover fresh paths and to pre- vent routing loops. The extended AODV is applied in using directions and positions of the source node and the destination node obtained from GPS to find routes. Basically, source and destination directions are used for the next hop selection. To do this, an intermediate node can be selected as the next hop in the requested route if it is located and moves in same direction as the source and/or destination. This modified AODV routing protocol uses the mobility model of nodes to support the various characteristics of sensor networks. This reactive protocol establishes updated routes only when required. However, the intermediate nodes could indicate inconsistent routes if the sequence number is not updated and, the idea to choose the next hop in same direction of source and destination does not guarantee the optimality of the route found. In addition, the network can be flooded by multiple RREQ and RREP in addition to unnecessary bandwidth consumption due to periodic beaconing. These works focus on deterministic multipath routing strategies, i.e., the route computation is not changed under the same topology. The topology based routing is of limited performance compared with geographical based routing. It requires additional node information during routing decision process. Because of high mobility in nodes. The topology based algorithm fails to handle frequent path breaks between source and destination. The geographic based routing is a routing principle that relies on geographic position information. It is mainly proposed on wireless network and based on the idea that the source node sends a message to the geographic location of the destination instead of using the network address. Geographic routing requires that each node can determine its own location and that source is aware of the location of destination. With this information a message can be routed to the destination without the knowledge of the network topology or a prior route discovery.

However, most previous works consider only network security and lifetime it does not consider about delay and packet delivery, which is one of the critical issues in WSNs. This work, jointly consider end-to-end delay and higher packet delivery that aim at designing an efficient hybrid priority based scheme which assure secured packet transmission with minimum delay and higher packet delivery of WSNs.

PROBLEM FORMULATION

A WSNs with sensor nodes are uniformly and randomly distributed in a circular region of many-to-one high-density is considered. The secure efficient disjoint multipath routing scheme the packets are sliced and randomly distributes and delivers the shares all over the network. This consists of two phases 1) formulation of optimization problem as the secret-sharing based multipath routing problem. In this routing scheme it deliver the sliced packet shares along the disjoint randomly generated paths by the routing strategy 2) It jointly consider the network lifetime and security. In this first the packets are sliced into shares by (T, M)- threshold secret-sharing algorithm and in that scheme the shares are dispersed in certain region around the source node. By using least hop routing it transmits the shares to the sink node. The multipath routing is mainly used to exist between more than one network and it is used for spreading of traffic from the source node to the destination over multiple network. From the queuing theory it is determined that by increased sharing the overall utilization of the entire network is improved. It also provides much better overall network performance by allowing better sharing of the available network resources and also it consists of three components. The multipath calculation algorithm to compute multiple paths, multipath forwarding algorithm to ensure that packets travel on a specific path and end-host protocol that effectively uses the determined multiple path. By using multipath routing in dense network it leads to congestion ie., higher delay and packet loss. Therefore it is necessary to avoid congestion which affect the throughput of the network.

HYPR: HYBRID PRIORITY BASED ROUTING SCHEME

HyPR scheme is used to decrease the routing overheads frequently incurred by traditional routing protocols. HyPR disseminates the packet transmission in a random manner. In addition to that HyPR uses multiple paths simultaneously between the source and destination to send packets inorder to reduce the transmission time to decrease routing overhead and to increase packet delivery ratio. It a combination topology based and geographic routing. The topology based is their route instability because of the established route consists of nodes between the source and destination that are affected by the frequent path. High routing overhead is shared between nodes before transmitting data. Another one is limitation of topology information in the discovery of routes with a high latency and higher transmission delay. In geographical routing it is difficult in finding an optimal next hop node when searching the destination node that is it uses long path to transmit data. It have inaccurate node coordinates, occurance of inherent loops while applying routing scheme and frequent network portioning. Since both have some advantage and disadvantage, by combining these to routing schemes the packet transmission rate is increased. The topology based routing is applied when the network density is high and the geographical routing is used when network is not dense. The network density is used to determine the type of routing methods and this decision is made by the source node after estimating the density based on the number of nodes extracted from the position table. The number of nodes in the sub-network is superior to the threshold 'α' called density coefficient is calculated using (1) then topology based routing is applied otherwise geographical routing is applied.

$\alpha = TR / \beta$ ---- (1)

where α represents the number of nodes in the network , T R represents the transmission range and β is a parameter of the observer that specify the TR density.

HyPR is mainly used to avoid delay and packet loss in secured and energy efficient routing. The packet delivery is defined as the number of packets received by the destination and delay is defined as the average time taken between the generation of packet by the source and time taken by the destination to receive packet.

CONCLUSION

WSNs are still under extension, and the routing scheme designed so far for WSNs have consider only security and lifetime of the network it have not taken network delay and packet loss into consideration. In this paper the proposed hybrid priority based routing protocol guarantee minimum delay and high packet delivery in addition to security and lifetime in the network. This uses two procedure for dealing with varying density in the network. When the network density is low it uses geographical routing and when the network density is high it uses topology based routing. Furthermore it provides an acceptable normalized overhead load measure.

REFERENCES

[1] Lin .x, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A strong privacy- preserving scheme against global eavesdropping for ehealth systems," IEEE J. Sel. Areas Commun., vol. 27, no. 4, pp. 365–378, May 2009.

[2] Akyildiz .I.F, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Comput. Netw., vol. 38, no. 4, pp. 393–422, Mar. 2002.

[3] Liu.A, J. Ren, X. Li, Z. Chen, and X. Shen, "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," Comput. Netw., vol. 56, no. 7, pp. 1951–1967, May 2012.

[4] Li.N, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey," Ad Hoc Netw., vol. 7, no. 8, pp. 1501–1514, Nov. 2009.

[5] Shu.T, M. Krunz, and S. Liu, "Secure data collection in wireless sen- sor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

[6] Kim.M, E. Jeong, Y. C. Bang, S. Hwang, and B. Kim, "Multipath energy- aware routing protocol in wireless sensor networks," in Proc. IEEE INSS, Kanazawa, Japan, 2008, pp. 127–130.

[7] Challal.Y, A. Ouadjaout, N. Lasla, M. Bagaa, and A. Hadjidj, "Secure and efficient disjoint multipath construction for fault tolerant routing in wire- less sensor networks," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1380– 1397, Jul. 2011.

[8] Karlof.C and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Netw., vol. 1, no. 2, pp. 293–315, Sep. 2003.

[9] Sun.H.M, C. M. Chen, and Y. C. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in Proc. IEEE TENCON, Taipei, Taiwan, 2007, pp. 1–4.

[10] Johnson.D.B, D. A. Maltz, and J. Broch, "Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks," Ad Hoc Netw., vol. 5, pp. 139–172, Dec. 2001.

[11] Marina.M.K and S. R. Das, "On-demand multipath distance vector routing in ad hoc networks," in Proc. IEEE ICNP, Riverside, CA, 2001, pp. 14–23.

[12] Lou .Wand Y. Kwon, "H-SPREAD: A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks," IEEE Trans. Veh. Technol., vol. 55, no. 4, pp.

[13] Shokrzadeh.H, M. Mashaiekhi, and A. Nayebi, "Improving directional rumor routing in wireless sensor networks," in Proc. IEEE IIT, Dubai, UAE, 2007, pp. 108–112.

[14] Banka.T, G. Tandon, and A. P. Jayasumana, "Zonal rumor routing for wireless sensor networks," in Proc. IEEE ITCC, Las Vegas, NV, 2005, pp. 562–567.

[15] Wang.H, B. Sheng, and Q. Li, "Privacy-aware routing in sensor net- works," Comput. Netw., vol. 53, no. 9, pp. 1512–1529, Jun. 2009. e sensors," IEEE Trans. Veh. Technol., vol. 59, no. 5, pp. 2472–2484, Jun. 2010.