SURVEY ON DYNAMIC SOURCE ROUTING, ATTACKS AND COUNTER MEASURES IN WIRELESS SENSOR NETWORKS

Jagadanna[1], Shivakumar .V. Saboji[2]

[1]*M.Tech student, Computer Science and Engineering, BEC Bagalkot, Karnataka, India*
[2]*professor, Computer Science and Engineering, BEC Bagalkot, Karnataka, India*

Abstract

A wireless sensor network (WSN) in its simplest form can be defined as a network of low power, small size devices denoted as sensor nodes that can sense the environment and communicate the information gathered from the monitored field through wired or wireless links. The data is forwarded, possibly via multiple hops to a sink that can use it locally, or it is connected to other networks through a gateway. Data is aggregated and send to the base station either using conventional wired network or fixed wireless medium. Data aggregation is a process of gathering and aggregating the data using data aggregation approach [1]. The main aim of data aggregation technique is to collect and aggregate data in an energy efficient manner so that network lifetime is enhanced. WSNs often use many routing protocols, power management protocols and data dissemination protocols where the design is to energy awareness and how can save energy [2]. Easy deployment, fast communication and low maintenance are main advantage of wireless sensor network [3].

The paper describe, introduction to wireless sensor networks and its types the challenging issues in routing the packets in WSN, the basic working principle of Dynamic Source Routing (DSR), how intermediate nodes can perform diversion of path when they are compromised by attacker, then paper enhances the loop control logic and digital signature based route path to overcome the diversion of path problem. Various simulators are used for the implementation and analysis of dynamic source routing in WSN [4].

Keywords: *Data aggregation, Digital signature, Dynamic source routing, Wireless sensor network.*

----------***----------

1. INTRODUCTION

A sensor network is a group of specialized transducers with a communications infrastructure intended to monitor and record conditions at diverse locations [5, 6]. A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor outputs. The transceiver, which can be hard-wired or wireless, receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from the electric utility or from battery.

There are two types of wireless sensor networks

1.1 Homogeneous Wireless Sensor Networks

Sensor networks where all sensors have the same capabilities in terms of computation, communication, memory, power supply, reliability, etc. They have symmetric links means that if A can reach B then B can also reach A.

1.2 Heterogeneous Wireless Sensor Networks

Sensor networks where sensors with different capabilities, are deployed to form a network, in terms of computation, communication, memory, power supply, reliability, etc. They possess asymmetric links means if A reach B then B may not reach A due different capabilities of sensor nodes (radio range). Heterogeneous sensors can triple the average delivery rate and provide a five-fold increase in the network lifetime.

The design of routing protocols in WSNs is influenced by many challenging factors [7]. The following section summarizes some of the routing challenges and design issues that affect routing process in WSNs.

Node deployment: Node deployment in WSNs is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths. However, in random node deployment, the sensor nodes are scattered randomly creating an infrastructure. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation

Reconfiguring route: Sensor node can use their limited supply of energy, performing computation and transmitting the information in a wireless environment. Sensor node lifetime shows a strong dependence on the battery lifetime. In a multi hop WSN, each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

Fault tolerance: Some sensor nodes may fail or be blocked due to lack of power, physical damage or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. If many nodes fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection base stations.

Scalability: The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more. Any routing scheme must be able to work with this huge number of sensor nodes. In addition, sensor network routing protocols should be scalable enough to respond to events in the environment.

Network Dynamics: Most of the network architectures assume that sensor nodes are stationary. However, mobility of both BS's and sensor nodes is sometimes necessary in many applications. Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, in addition to energy, bandwidth.

2. DYNAMIC SOURCE ROUTING

DSR protocol is reactive or on demand protocol. Route is established only when there is demand for data transfer.DSR is completely self organizing and self configuring without the need for any existing network infrastructure or administration. DSR does not rely on functions like periodic routing advertisement, link status sensing and neighbor detection packets; this makes the number of overhead packets caused by DSR scales down to zero. DSR is designed specifically for use in multi hop WSN scenario. Source specifies entire route, it places the complete path to destination in message header. Packet forwarding logic is that the intermediate nodes read the path specified in header and places the packet on the next link to words the destination. Every node in the path to destination acts both as receiver and router to forward data to destination.

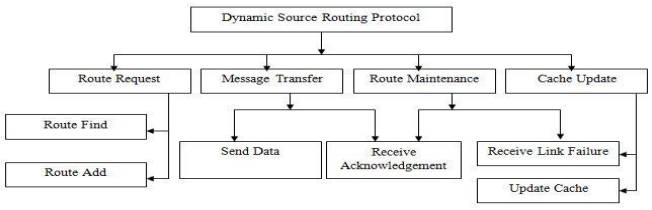

Fig -1: Architecture of DSR

It involves Route request transfer, Route reply, Routing caching, Data transfer, Route maintenance

2.1 Route Request Transfer

The sensor node (source) which has data that need to be sent to sink, first it will check its cache to find route to destination if found it will use that route to perform data transfer, if it does not then it will perform broadcasting of RREQ messages. Source broadcast RREQ request to its neighbors. The RREQ request contains the source address, destination address, unique request id. The neighbor node compare their address with the destination address if matches provide route reply to source if does not match then node inserts the node id in to RREQ request header and further broadcasts to its neighbors, this process repeats until the destination or sink is reached. The nodes that have already broadcasted RREQ request may get the RREQ message from other neighbor nodes but those not broadcasted again; those packets are discarded based on the request id of the RREQ message.

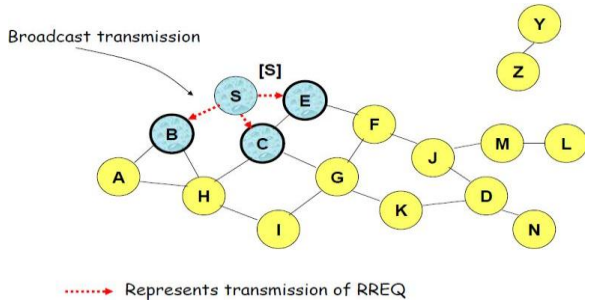

Fig -2 a

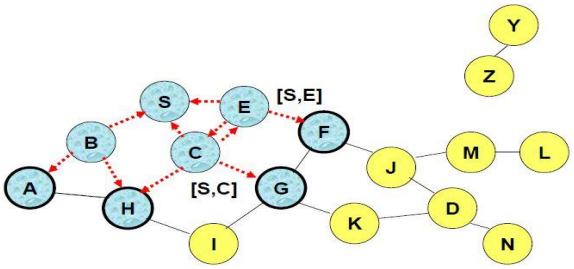

Fig-2.b

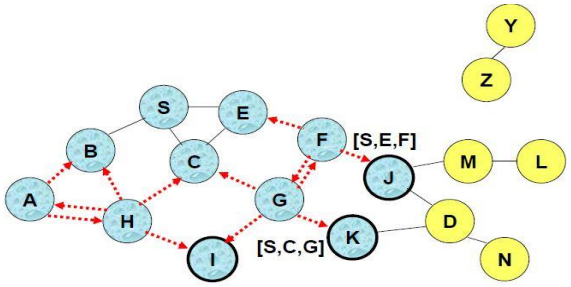

Fig -2.c

Figure 2.a shows source S broadcasts route request RREQ to its neighbors B, C and E. Fig 2.b shows the sensor nodes B, C and E inturn broadcast the RREQ message to its neighbors as shown in Fig 2.c

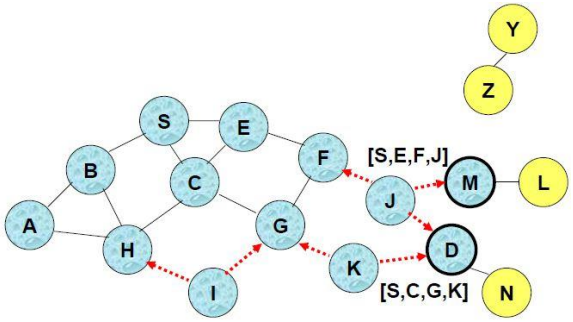

Fig -2.d

Fig -2: Broadcasting of route request RREQ.

Figure 2.d shows finally the RREQ route request reaches the destination D.

2.2 Route Reply

Once the RREQ request message reaches the destination or sink, the request message header will have information about the intermediate nodes that it is has travelled. Using this path information the sink sends reply RREP message conveying route information to source. Sink sends unicast message to source about the path that need to be adopted to have data transfer between sink and source.

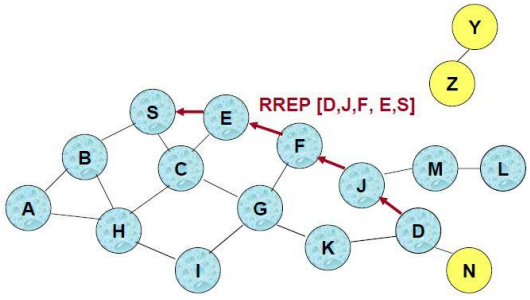

Fig -3: RREP route reply transfer.

2.2.1 Route Reply Storms

When multiple nodes have routes for destination then it can create Route Reply Storms which also result in collisions of control packets and increase congestion at that node where reply is sending. [8] Suggests solution that is introducing delay before sending reply. Route reply coming from different hop length so reply from short hop length will comes first.

$$Delay = H * (h-1+r)$$

Where delay is time for pausing the reply H is any constant delay introduce per hop, h is total number of hops involve to reach destination node, r is random number.

2.3 Data Caching

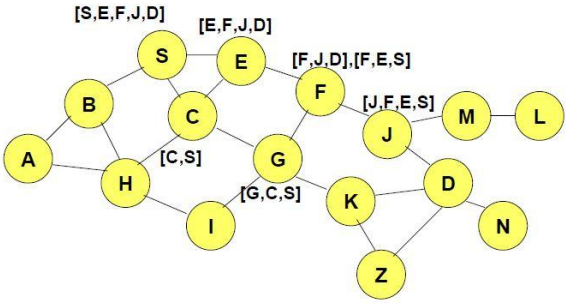

Fig -4: DSR route caching.

When source gets the route reply it will store that route in its cache and use that path preferably to perform data transfer. The nodes in sensor networks learn route to other nodes either through route request RREQ messages or route reply RREP message.

2.4 Data Transfer

Source knows the route to sink, it puts entire information about route to sink in packet header and forward it to the next hop node in the path.

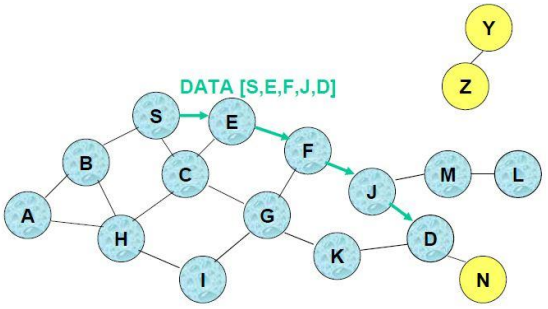

Fig -5: DSR data transfer

Intermediate nodes read the path specified and forward accordingly until the packet reaches the destination.

2.5 Route Maintenance

In WSN the node and link failure very often that may lead to dynamic change in routes or the network topology. Source when sends packet it will wait for acknowledgement from destination within a specified time interval, if does not get acknowledgement then it will consider as one of the nodes in the path to destination has goes down and uses the other available paths to perform data delivery.

3. VARIANTS OF DSR

Route discovery may yield number of routes to destination. Consider the shortest path to destination minimizing total transmission energy and load sharing approach[9].The main disadvantage of the first protocol is that the nodes along the paths 'die' very soon in compare to other nodes so consider avoiding over utilized nodes while selecting a routing path. A node determines whether to forward the route-request message or not, depending on its residual battery energy. If it has energy level higher than a threshold, node forwards the route request message; otherwise it drops the route request message. In ESDSR, the node which has a tendency to die out very soon is avoided during the route discovery phase of this protocol. Alternate solution for load balancing can also be achieved by considering multiple paths to destination and make use of all available to transfer data to destination so the chances of node tendency to die out soon in shortest path protocol consideration can be overcome. In [10] the protocol achieves increased reliability through the maintenance of a reliability factor by the nodes in the network. During the route discovery process, the request messages are only propagated to nodes with a reliability (usually the battery energy) factor that is above a threshold value specified by the application. Different methods for the maintenance of the reliability factor by the nodes, as well as other optimizations to enhance network performance and reduce path discovery overhead are introduced. [11] Proposes multipath source routing, use multiple paths for the same destination to route the packet. DSR's route discovery mechanism that returns multiple paths is employed in MSR. All the routes discovered are stored in the route cache with a unique route index for each. So it is easy for us to pick multiple paths from the cache. An option can also be added to the MSR for optimization, allowing the packets distribution to be rescheduled in the intermediate nodes according to their local multipath load distributing processes, if the intermediate nodes have paths to destination and they would like to do so. This forms the cascaded multipath routing, which makes full use of network resources achieving stronger load balancing approach without additional network overhead. When multipath is considered for data transfer some of the route may be lengthy. In DSR entire route to destination is part of the data packet, route become lengthy as no of intermediate node in route increases. [12] Eliminate the lengthy route in packet header and introduces unique flow id for each flow on a particular link to carry data from source destination using IPv4 and IPv6 maintaining the required QoS. A data packet contains source address, destination address, and flow identifier replacing entire the intermediate path information. Intermediate node will retain soft state of the information which indicates the next hop. Each packet will be forwarded without having to take the entire source route on the packet header. The Nodes in WSN are often prone to failure. [13] Proposes Dynamic Source Route Link Switch mechanism (DSR-LS) to detect link failure in advance and adopt new link and avoids the route discovery process conserving the node energy and enrich network life time. It detects a link breakage trend based on power of arrival packets. Then DSR-LS send a link switch request (LSRE) in one-hop range to search appropriate nodes acting as relaying stations. By this local link-switch method, a route can be shift to a more stable path. The entire above discussion only one sink in considered but it is possible to have multiple sinks and all receiving the same data in energy efficient way Aggregation Overlay Multicast (AOM) protocol [14]. That helps to decrease energy consumption while a source sends a packet to multiple destinations or sinks by choosing possible common path then unicast to each destination node. In overlay multicast the idea is to transmit multicast messages as unicast messages between group members. Replication of the messages to multiple members is done only at the branching member nodes. The member nodes, together with the logical unicast links between them, form an overlay network. The intermediate member nodes prepare their own header and relay the message through source routing. To improve the route maintenance DSR uses two levels of thresholds [15]. The higher level of threshold is used to find the optimal fresh back-up route from source's route cache, if available. If there is no fresh route, then source starts new route discovery before actual breakage of primary route. At the lower level of threshold, 'S' either uses fresh back-up route as primary route or buffer all data packets till new route discovered. By analyzing E-DSR, we get that EDSR decreases the number of dropped data packets i.e. increases the PDF packet delivery fraction) and reduces average end to end delay.

4. DSR ATTACKS AND COUNTER MEASURES

This section discusses few attacks on DSR and suggests possible solutions. Many sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to attacks [16]. Most network layer attacks against sensor networks fall into one of the following categories: Spoofed, altered, or replayed routing information, Selective forwarding, HELLO flood attacks, Acknowledgement spoofing. Public key cryptography is too expensive for sensor nodes. Security protocols for sensors networks must rely exclusively on efficient symmetric key cryptography. A secure routing protocol should guarantee the integrity, authenticity, and availability of messages in the presence of adversaries of arbitrary power. Every eligible receiver should receive all messages intended for it and be able to verify the integrity of every message as well as the identity of the sender. [17] Presents a probabilistic attack model on the DSR protocol and analyses its effect on the DSR routing performance. The attack is catastrophic only if a large number of nodes are compromised and there is no detection mechanism. When an attacker who has captured a normal node receives a route request packet, it checks if there exists a route to the destination in the route cache. If yes, it sends the route reply with probability 1-P (forces to select possible worst path) else the attacker does not broadcast route request or rebroadcasts

with probability 1-P. attackers aim to disrupt the route discovery with the maximum effect without being detected and will not be detected until he compromises a certain number of nodes and/or increases the attack probability. To solve this watchdog and pathrater are introduced in DSR. When a node forwards a packet, the node's watchdog verifies whether the next node in the path also forwards the same. If the next node does not forward the packet, then it is misbehaving .The pathrater assesses the results of the watchdog and selects the most reliable path for packet delivery. DSR suffers from resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes battery power [18]. These attacks are called as vampire attacks. These Vampire attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. All protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O (N), where N in the number of network nodes. The paper suggests loop control logic to overcome from carousel attack but fails to control the stretch attack that can be detected and prevented by the usage of digital signature. Even though the attack is detected the paper neither suggests any procedure for a compromised sensor node to recover nor any action against the attacker.

FUTURE ENHANCEMENT

Even if some nodes in the routes are compromised, Even though the alternate route is selected for data transfer that may also suffer from threat to be attacked. At some stage if N number of sensor nodes are compromised then it leads to the failure of whole sensor network. The sensor nodes should defend against the attack, and there should some recovery mechanism even if some nodes are compromised and some action should be taken against the attacker to reduce the strength of the attack on sensor network.

REFERENCES

[1] P. N. Renjith and E. Baburaj, "an analysis on data aggregation in wireless sensor networks", 2012 International Conference on Radar, Communication and Computing (ICRCC), SKP Engineering College, Tiruvannamalai, TN, India. 21 – 22 December, 2012. pp.62-71.978-1-4673-2758-9/12/$31.00 ©2012 IEEE.

[2] Jamal N. Al-Karaki Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", ICUBE initiative of Iowa State University, Ames, IA 50011.

[3] J.M. van Dam, "An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks", parallel en gedistribueerde systemen, June, 2003.

[4] Marko Korkalainen, Mikko Sallinen, Niilo Kärkkäinen, Pirkka Tukeva, "Survey of Wireless Sensor Networks Simulation Tools for Demanding Applications", Fifth International Conference on Networking and Services, 2009.

[5] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networkS: A survey", ELSEVIER, Computer Networks 38 (2002) 393–422.

[6] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal , "Wireless sensor network survey", ELSEVIER, Computer Networks 52 (2008) 2292–2330.

[7] Kemal Akkaya and Mohamed Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", ELSEVIER, Ad Hoc Networks 3 (2005) 325–349.

[8] Shakeel Ahmad, Irfan Awan, Athar Waqqas and Bashir Ahmad, "Performance Analysis of DSR & Extended DSR Protocols", Second Asia International Conference on Modeling & Simulation.

[9] Mohammed Tarique, Kemal E. Tepe, and Mohammad Naserian, "Energy Saving Dynamic Source Routing for Ad HocWireless Networks", Electrical and Computer Eng. Dept. University of Windsor Windsor, Ontario N9B 3P4, CANADA.

[10] Imad Jawhar, Zouheir Trabelsi, and Jameela Al-Jaroodi, "Towards More Reliable Source Routing in Wireless Networks", International Conference on Networking, Architecture, and Storage.

[11] Lei Wang, Lianfang Zhang, Yantai Shu and Miao Dong, "Multipath Source Routing in Wireless Ad Hoc Networks", Department of Computer Science, Tianjin University Tianjin 300072, China.

[12] Wai Yee Tai, Chong Eng Tan, Sei Ping Lau, "Towards Utilizing Flow Label IPv6 in Implicit Source Routing for Dynamic Source Routing (DSR) in Wireless Ad Hoc Network", Department of Computer Systems and Communication Technologies, Faculty of Computer Science and Information Technology, University Malaysia Sarawak, Malaysia.

[13] Hongsheng Lu, Jun Zhang, Xiling Luo, "Link Switch Mechanism based on DSR Route Protocol", First International Conference on Intelligent Networks and Intelligent Systems.

[14] Chi-Kuo Chiang, Chung-Ta King, "Source Routing for Overlay Multicast in Wireless Ad hoc and Sensor Networks", Department of Computer Science, National Tsing Hua University.

[15] Chiranjeev Kumar, Gourav Kumar, and Puja Rani, "Efficient-Dynamic Source Routing (E-DSR)", 2012 international symposium on communication and information technologies.

[16] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley.

[17] Jaydip Sen, "An Analysis of Routing Disruption Attack on Dynamic Source Routing Protocol", Innovation

Lab, Tata Consultancy Services Ltd.Bengal Intelligent Park, Salt Lake Electronic Complex Kolkata 700091, INDIA.

[18] Eugene Y. Vasserman and Nicholas Hopper, "Vampire attacks: Draining life from wireless ad-hoc sensor networks", IEEE Transactions on Mobile computing, Volume: 12, Issue: 2, Issue Date: Feb, 2013.

BIOGRAPHIES

Mr. Jagadanna was a staff Bheemanna Khandre Institute of Technology, Bhalki (Formerly known as Rural Engineering College) and currently perceiving PG degree in Computer Sceince and Engineering at Basaveshwar Engineering College Bagalkot-587102, Karnataka, India

Dr. Shivakumar . V. Saboji has perceived his Ph.D from VTU university on "Vertical Handoff System in 4G Wireless Networks" and currently working as professor in Computer Science and Engineering at Basaveshwar Engineering College Bagalkot-587102, Karnataka, India