International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 6, June-2015, pp: (82-85), Impact Factor: 1.252, Available online at: www.erpublications.com

A Review on Sensor Security and Power Optimization in AODV

Agraj Bhandari[1], Nidhi Sood[2]

[1]M.Tech Scholar, Bahra University, Shimla, India
[2]Assistant Professor, Deptt. of Computer Science and Engineering, Bahra University, Shimla, India

---

Abstract: Wireless sensor networks are becoming more and more popular these days because of their large range of applications. These networks are used in many fields like to examine environmental conditions, forest fire detection, battlefield surveillance, water level monitoring and in many other applications. These sensors are deployed over a very larger area. Hundreds or even thousands of sensors are placed over harsh and remote environments where providing electrical power is very difficult. So these devices are operated on batteries. And as we know that the power of a battery is limited. So there is a need of using some techniques and protocols that help to increase the battery life. Another important part is the security of nodes. It is highly recommended that no data can be stolen by any intruder. Data should be transferred to the sink node in a secure way. Ad-hoc-On-Demand Distance Vector (AODV) protocol is one of the most widely used protocols and is undergoing extensive research and development. AODV protocol was a good traditional approach but it does not provide any security measures and power optimization techniques. In this study some modifications are made that will enhance its properties.

Keywords: Ad-hoc-On-Demand Distance Vector (AODV).

Introduction

The wireless sensor network is the network that senses environmental conditions like temperature, pressure, humidity etc. and passes this information to the sink node. A WSN is comprised of very large number of nodes and one or more sink nodes. The nodes mainly use a broadcast communication and the network topology can change constantly. These kinds of devices have limited power, low computational capabilities and limited memory. These battery powered nodes are typically unattended because of their deployment in harsh and remote environments. A number of power saving techniques must be used both in the design of electronic transceiver circuits and in network protocols. The first step towards reduced power consumption is a sound electronic design, selecting the right components and applying appropriate design techniques to each case. Energy loss is caused by several activities. One of the major activity is when the sensor nodes transmit data from source to destination. Another major issue in WSN is the sensor security. There are several attacks possible. The main attack in the network layer is the "Man In the Middle Attack". This attack is performed while a node selects another node while transmitting the data. Here an attacker can act as a genuine node and can hack into the ongoing transmission process.

Routing protocols for Mobile Ad Hoc Networks can be broadly divided into two distinct categories, **namely Proactive (table-driven) routing protocols and Reactive (on-demand) routing protocols.** In **Proactive Routing protocols**, each node maintains up-to-date routing information to every other node in the network. Routing information is kept in a number of routing tables and updates to these tables are periodically. **Reactive or On-demand routing protocols** are designed to overcome the increased overhead problem in proactive protocols. Unlike proactive protocols, reactive protocols create a route only when desired. If a node desires to send a message to a destination node for which it does not have a valid route to, it initiates a route discovery to locate the destination node. The process is completed when a source node finds a route to the destination. AODV is a widely used reactive protocol. The main objective of this paper is to modify the existing AODV protocol for energy optimization and security techniques.

AODV Protocol

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes.

AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it.

As the RREP propagate back to the source, the nodes sets up the forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route.

As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination. After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

Drawbacks of AODV Protocol

The main drawbacks of AODV Protocol are:

1. In AODV, very less amount of information of the neighbours is shared. The information contains: Sequence Numbers, Hop count, Neighbour Node's Ip.
2. In AODV, the security that is being provided to the nodes is very less. Hence it is very prone for Man In Middle Attack.

Related Work

Prashant Kumar, Gaurav Sharma had done extensive study on the AODV protocol and concluded that AODV transmits network information only on-demand. AODV can gather only a very limited amount of routing information, route learning is limited only to the source of any routing packets being forwarded. The limited proactive part is the route maintenance (HELLO messages). The AODV protocol is loop-free and avoids the counting to infinity problem by the use of sequence numbers. This protocol offers quick adaptation to mobile networks with low processing and low bandwidth utilization. The weaknesses of AODV include its latency and scalability.

Anu Arya, Jagtar Singh had done comparative study of various proactive and reactive protocols and concluded that performance of AODV protocol is far better than proactive protocols as it reduces the information overhead.

Charles E. Perkins and Elizabeth M. Royer

They had done their study to show that AODV can find routes quickly and accurately. They concluded that:-

- Nodes store only the routes that are needed
- Quick response to link breakage in active routes

- Loop free routes maintained by use of destination sequence numbers
- Scalable to large populations of nodes

Shancang Li, Member, IEEE, Shanshan Zhao, Xinheng Wang

They had developed an adaptive load-balancing multipath routing protocol (SM-AODV) for WSNs that uses load balancing, congestion control, and secure delivery scheme to address the limitations in existing multipath routing schemes. InSM-AODV, the packets are delivered across multi paths using a secure and reliable scheme, which decouples the node's capabilities SM-AODV achieves substantial reliability improvement in routing downstream traffic by using a secret sharing scheme at the source. SM-AODV adopts an adaptive congestion control scheme, which is effective even in the case that node or link failure occurs frequently

Sandra Sendra, Jaime Lloret, Miguel García

They had presented the main causes of energy loss in wireless sensor nodes. The main characteristics required to make a wireless sensor node and the factors to be considered when implementing a WSN or ad-hoc network have been discussed. They discussed energy wastage given by the electronic circuit. Therefore, counting on a sound electronic design that includes the right components for the sensor device is absolutely essential.

Chiara Buratti, Andrea Conti, Davide Dardari and Roberto Verdone

They discussed some of the most relevant issues of WSNs, from the application, design and technology viewpoints. For designing a WSN, in fact, we need to define the most suitable technology to be used and the communication protocols to be implemented (topology, signal processing strategies, etc.). These choices depend on different factors, above all the application requirements.

Problem Formulation

Since AODV is one of the widely used reactive protocol but there are always some fields where enhancement can be done for better results. Since in AODV protocol, a route is created only when it is needed. But in AODV there is very less amount of route information is provided for the neighbor nodes like neighbor IP, Sequence number and hop count.

The main motive of his research is to enhance the information that is being shared among the nodes so that AODV will consider some more parameters while selecting the nodes for the transmission. AODV always chooses its path according to the traditional parameters like minimum number of hops and higher sequence number. Every time it chooses its path according to these parameters. The main problem comes here. Suppose if the data is to be transferred again and again from source A to destination D, the AODV will repeatedly chose the same path according to lesser number of hops and higher Sequence number. This results in the reduced battery life of the sensors that are being used for the transmission. And after some time the sensors will not be able to work because of less power. The main idea behind this research is to make the paths dynamic by adding some more parameters to the information of nodes that is shared while transmission process. By adding new parameters, the AODV will consider more parameters not only the traditional one while selecting the nodes for the transmission. This will enhance the battery life of the nodes as the nodes will be used in a dynamic manner. Also the security of the nodes is to be optimized by adding some of the new parameters.

Conclusion

The main conclusion of this research is to remove the drawbacks of AODV protocol like security and power issue of the nodes. In this proposed research the enhanced AODV protocol will choose a dynamic path by considering the new factor that is being added to the information of nodes that is shared while selecting the node for transmission. By choosing the dynamic path the AODV will overcome the two drawbacks. First, it will enhance the battery life of nodes as the same nodes will not be chosen again and again. By doing so, it will help other nodes to get recharged from natural phenomenon as they are in idle state. Second, by choosing dynamic path, it will not be an easy task for the intruder to crack the transmission path, as most of the attacks are pattern attack. Hence the proposed research will try to overcome these issues.

References

[1]. Prashant Kumar Maurya, Gaurav Sharma,VaishaliSahu, Ashish Roberts, MahendraSrivastavaVol.1, No.2, November 2010 DOI : 10.5121/ijcses.2010.1206 63.
[2]. C. E. Perkins, E. M. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, July 2003.IEEE Computer Society, "IEEE 802.11 Standard, IEEE Standard For Information Technology," 1999.
[3]. Power saving and energy optimization techniques for Wireless Sensor Networks Sandra Sendra, Jaime Lloret, Miguel García and José F. Toledo Universidad Politécnica de Valencia Camino Vera s/n, 46022, Valencia, Spain.
[4]. Dynamic Channel Assignment for Wireless Sensor Networks: A Regret Matching Based Approach Jiming Chen, Senior Member, IEEE, Qing Yu, Bo Chai, Youxian Sun Yanfei Fan, Sherman Shen, Fellow, IEEE.
[5]. Comparative Study of AODV, DSDV and DSRRouting Protocols in Wireless Sensor Network, AnuArya, Jagtar SinghAnuArya / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014.
[6]. Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks Shancang Li, Member, IEEE, Shanshan Zhao, Xinheng Wang, Member, IEEE, Kewang Zhang, and Ling Li.