Improved Energy Efficiency Hybrid Protocol In Wireless Sensor Network

Jyoti Raheja, Dr. Sandeep Singh Kang

Abstract— Wireless sensor network (WSN) is useful supplement to the modern wireless communication networks**.** New advancement in wireless sensor networks have emerged to many new protocols which are specifically designed for sensor networks where energy awareness is an essential consideration. In this work proposing energy efficient secure routing protocols. Three main protocols explored in this paper are WBAODV, DSR and Hybrid. We are proposing the WBAODV and DSR Protocol to make the hybrid approach in the sensor network. Result obtained by simulation campaign shows that Hybrid protocol has some important advantages that make it a valuable and to be particularly suitable in environments where high throughput and less end to end delay is requested. Current protocol will also be tested under malicious node attack. Performance Results will be analyzed with following performance Matrices, in terms of Throughput, Packet Delivery Fraction and End to End Delay.

Index Terms— DSR, Hybrid, WBAODV, Wireless Sensor Networks

1 INTRODUCTION

WSN is a network consists of hundreds or thousands of wireless sensor nodes which collect the information from their surrounding environment and send their sensed data to sink node. Wireless Sensor Networks have critical applications in the scientific, medical, commercial, and military domains [5]. Examples of these applications include industrial monitoring, data logging, landslide detection and offices, observation of water quality, and intelligent transportation systems. Wireless sensor network also has significant usages in area monitoring. The challenge in WSNs is to maximize the lifetime of sensor nodes with sensing capabilities [3] because practically it is not possible that one can replace the batteries of large no of deployed sensor in the environment. We focus on data routing problems in energy constrained sensor networks.

2 ROUTING PROTOCOLS

A routing protocol uses software and routing algorithms to determine optimal network data transfer and communication paths between network nodes. Routing protocols facilitate router communication .In WSN; the routing protocols are data centric, application specific, capable of aggregating data and capable of optimizing energy consumption. The important characteristics of a good routing protocol for WSN are its simplicity, energy awareness, scalability and adaptability due to limited Energy supply, limited power of computation, requires limited memory and limited bandwidth of WSN.

Routing protocols are divided in to three parts, First one is Proactive i.e. Table Driven, second is Reactive i.e. On-Demand and Hybrid protocols [4] and they depends on how the source finds a route to the destination. In Pro-active protocols sensors advertise their routing state to the entire network to maintain a common (partially) complete topology of the network. Examples of such schemes are the Destination Sequenced Distance Vector (DSDV). On the other hand, Reactive protocols depends upon request an establish path, e.g. in response to a query, or an event, meanwhile, sensors remains idle in terms of routing behavior. Sensors forward each routing request to peers until it arrives at a sink. The latter will respond over the reverse communication path. Examples of reactive routing schemes are Adhoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR). Hybrid protocols use a combination of these two ideas.

2.1 DSR Dynamic source routing protocol (DSR) is an on-demand protocol. It is designed to restrict the bandwidth i.e. consumed by control packets in wireless networks by eliminating the periodic table-update messages i.e. required in the table-driven approach. DSR is beacon-less [5] compare to other on demand protocol and hence does not require periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbors of its presence. In DSR all the routing information from the source to the destination is included in the header of the request.) If any link failure occurs in the network, DSR send a unicast packet [7] to the source

giving the information about the broken link. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding RouteRequest packets in the network. When the destination node, receives a RouteRequest packet, it responds by sending a RouteReply packet back to the source.

2.2 AODV: The AODV Routing protocol [7] uses an on-demand approach for finding routes, as each node maintains a routing table that contains routing information to all the nodes in the network. If any link failure occurs in the network, AODV broadcast the Route error message to all its neighbors as it is possible that the reverse path from the problematic node to the source has timed out The major difference between AODV and Dynamic Source Routing (DSR) is how to resolve the problem if caches with information are outdated or broken. The problem of stale caches in DSR is solved by stopping the response from the intermediate host if the reply packet causes a loop formation. Figure 1 shows AODV handles this problem by maintaining a sequence number in the route table. This sequence number corresponds to the freshest route available to the destination. More the sequence number fresher is the route. So now if the link fails, the node which was joined to the link and the network broadcast a route error with increased sequence number. So no node which has lesser sequence number than the received sequence number will respond using its local cache.

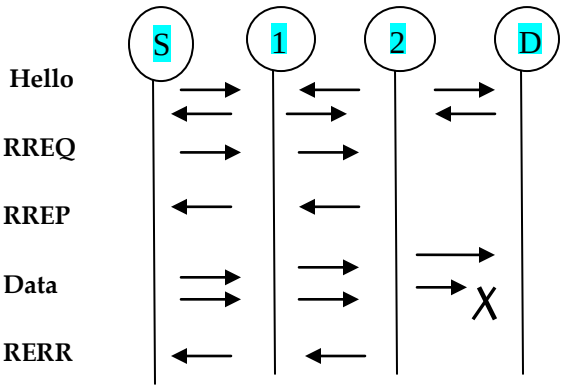


Fig 1 Process of AODV

2.3 Hybrid This protocol [7] depending on how the source finds a route to the destination. Hybrid protocols use a combination of these two ideas (WBAODV&DSR).These two combine to form WBAODVDSR.

3 PROPOSED SCHEME

The AODV Routing protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packet. DSR uses source routing in which a data packet carries the complete path to be traversed. The WBAODV is weight based [3] AODV protocol to enhance the stability of a network. The WBAODV and DSR combines to form a WBAODVDSR .Figure 2 shows the hybrid mechanism that act as efficiency in sensor network. Then check where protocol may act better .If WBAODV is acting good as energy efficiency use WBAODV, if DSR is good use DSR and if both are acting as same at same place then use much more.

- Traffic
- Long Distance
- Bandwidth
- Congestion

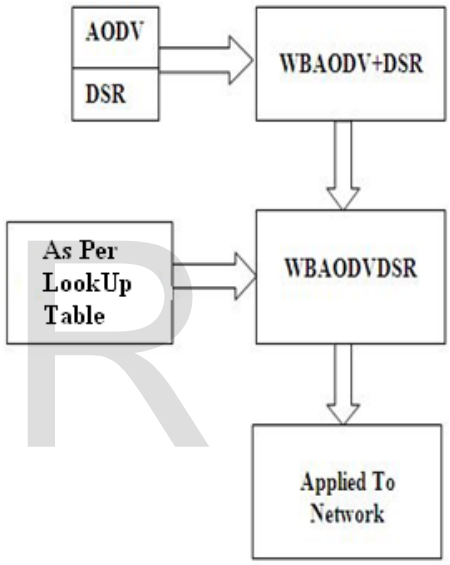


Fig. 2 Hybrid mechanism of sensor network

Algorithm:

- Create the agent.
- Look up communication variables.
- Create a service to start up look up process.
- Repeat the process up to 100 nodes and scanned based on the congestion complexity of the path and bandwidth.
- We choose Select S1: WBAODV, S2: DSR.
- If there is congestion or low bandwidth, we choose DSR.
- For energy consumed at long distance, we choose WBAODV.

Malicious Node: There are basically two a different type of attacks one is active attacks and other is passive attacks [1].

WSN attacks can be identified as external and internal attack according to the domain of attacks Sometimes both reviews are applied, such as "internal active attack," "internal passive attack," etc. will be used to highlight the type of an attack. In Active Attack attacker transmits data to one or both of the nodes in the communication channel. Active attackers can disrupt the normal functionality of the whole network, which means it may change the original information or modify the original data. On the other hand, passive attacks are those which attacks indirectly are mainly due to lack of cooperation and save the energy selfishly. Malicious Nodes that perform active attacks have the aim of damaging other nodes by causing network .Malicious attack appears in the form of code, scripts, active content, and other software. Malicious attack includes computer viruses, worms, Trojan horses, root kits, key loggers, dialers, spyware etc. It mainly attacks at the backdoor. A backdoor is a method of bypassing normal authentication procedures. Once a system has been compromised, one or more backdoors may be installed in order to allow easier access in the future. Backdoors may also be installed prior to malicious software, to allow attackers entry.

4 SIMULATION PARAMETERS

To evaluate the performance of wireless sensor network we evaluate the Ratio of received to sent(r/s) with the help of received parameter and send parameter.

4.1 Packet Delivery Fraction-It is the ratio of data packets delivered to the destination to those generated by the sources. It is calculated by dividing the number of packet received by destination through the number packet originated from source.

$$PDF = \left({}^{P_r}/_{P_s}\right) * 100$$

Where P_r total Packet is received & P_s is the total Packet sent.

4.2 Average End-to-End Delay (millisecond)-This includes all possible delay caused by buffering during route discovery latency, propagation and transfer time. It is defined as the time taken for a data packet to be transmitted across a WSN from source to destination.

$$D = (T_r - T_s)$$

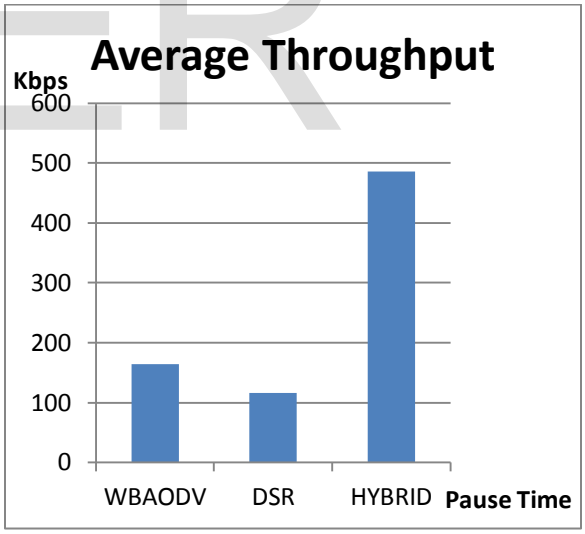
Where T_r is receive Time and T_s is sent Time

4.3 Throughput-The throughput of the protocols can be defined as percentage of the packets received by the destination among the packets sent by the source. In this case throughput is measured by revenue received (or not) at the point of sale—exactly the right time. It is measured in kbps.

5 RESEARCH WORK

There are many research papers on routing protocols in wireless sensor network and all are used for evaluating performance of different parameters in different scenario. Researchers specify the performance for different parameters and which one is best for the case of Wireless Sensor Network. In comparison of AODV, DSR and Hybrid the Average end-to-end delay of WBAODV is very high. While in comparison of DSR and WBAODV routing protocols, WBAODV performed better than DSR in terms of throughput. As compare to WBAODV and DSR, Hybrid protocol perform better which has high Throughput and less End To End delay and high pdf.

Performance Comparison Based Upon Throughput:
Throughput refers to the ratio of the amount of packets received at the Destination to the amount of packets transmitted at the Source. This value should be higher, to increase the performance of the network. Throughput of Hybrid is high when compared with WBAODV and DSR



.

Performance Comparison Based Upon End to End Delay:
End-to-end delay is defined as the time taken for a data packet to be transmitted across a WSN from source to destination. End to End Delay is calculated by:

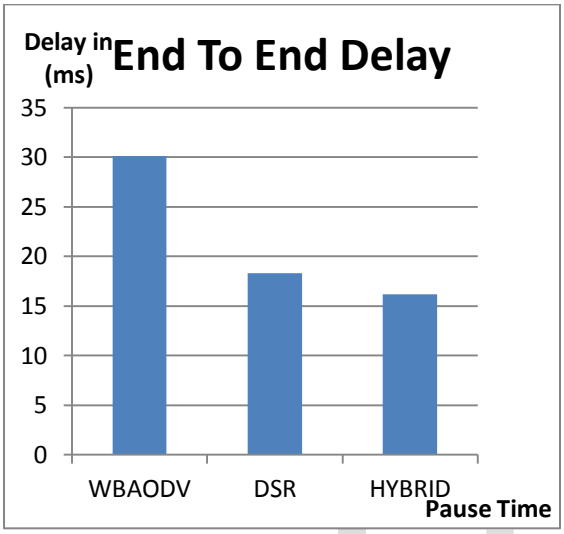
$d_{end\text{-}end} = N[\, d_{trans} + d_{prop} + d_{proc}\,]$ where

$d_{end\text{-}end}$ = end-to-end delay

d_{trans} = transmission delay

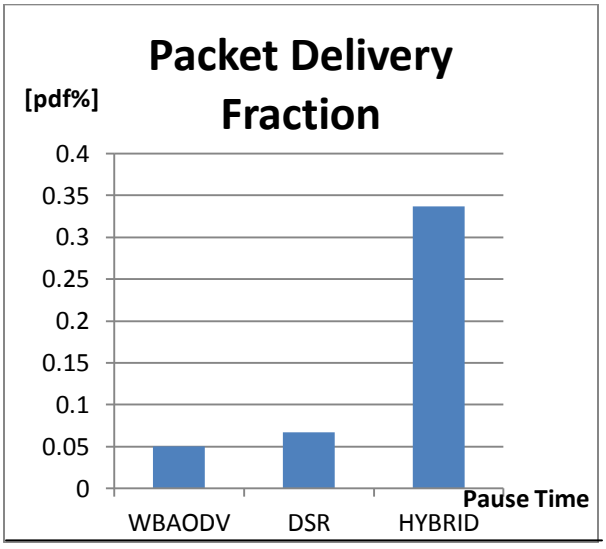
d_{prop} = propagation delay
d_{proc} = processing delay

End to End delay of WBAODV is high than DSR and Hybrid.



***Performance Comparison based upon Packet Delivery Fraction*:**

It is the ratio of data packets delivered to the destination to those generated by the sources. It is calculated by dividing the number of packet received by destination through the number packet originated from source. Packet delivery fraction of DSR is higher than WBAODV. Packet delivery fraction of Hybrid protocol is highest than both of DSR and WBAODV.



6 CONCLUSIONS

This paper proposed an Energy Efficient date routing technique for the Wireless Sensor Networks, by using the WBAODV, DSR and HYBRID routing protocol. Results of proposed technique with Hybrid give better results under attacks condition in WSN. In future more attacks can be simulated and check the performance of the proposed hybrid protocol. We shall also propose the multicast protocol for large network.

ACKNOWLEDGEMENT

I express my sincere gratitude to the Punjab Technical University, Jalandhar for giving me the opportunity to work on the thesis during my final year of M.Tech.
First of all I am thankful to our project guide Dr. Sandeep Singh Kang, HOD, Computer Science and Engineering Department, CGC College of engg, Landran under whose guideline I was able to complete my thesis. I am wholeheartedly thankful to him for giving us their valuable time and attention and for providing us a systematic way for completing my project.
I must make special thanks of faculty members for their co-operation and assistance in solving problems. I would like to thank our Head of department, Mr. Rajwinder Singh, Computer Science and Engineering Department and all assistants for providing us assistance in various hardware and software problem encountered during course of our project.
Thesis work is an important aspect in the field of engineering. I would also like to thank my parents, friends etc who helped me in my thesis.
I would also like to thank everyone who has knowingly & unknowingly helped me throughout my thesis. Last but not least, a word of thanks for the authors of all those books and papers which I have consulted during my thesis work as well as for preparing the report.

REFERENCES

[1]A.Rajaram,S.Palaniswami(2010),"Malicious Node Detection System for Mobile Adhoc Networks", International Journal of Computer Science and Information Technologies, Vol. 1, 2010, pp.77-85

[2]Rajaram.A,Palaniswami,S.(2010),"Malicious Node Detection System for Mobile Ad hocNetworks", International Journal of Computer Science and Information Technologies, Vol. 1 (2) ,pp.77-85

[3] Christina, Edvinoe. And JothiChitra, R. (2011), "*Energy Efficient Secure Routing in Wireless Sensor Networks*", Proceeding of ICETECT, pp.982-986

[4] K.Prabhat, M.P.Singh and U.S.Triar (2012), "A Review of Routing Protocols in Wireless Sensor Network" *International Journal of Engineering Research & Technology* (IJERT) ,vol. 1, Issue 4.

[5] Lal Dua, R. and Sharma,M.(2012), "*Comparison Of Different Routing Protocols (DSR & AODV) On Behalf Of Evaluation of Different routing parameters with constraints"*, International Journal of Computer Networks and Wireless Communications, vol.2, pp.408-413

[6] Singh, G. and Singh, A. (2012) "*Performance Evaluation of Aodv and Dsr Routing Protocols for Vbr Traffic for 150 Nodes in Manets"*, International Journal Of Computational Engineering Research, Vol.2, issue.5,pp. 1583-1587

[7] S.Ganesh, Amutha.R (2012), "Efficient and Secure Routing Protocol for Wireless Sensor Network using Mine detection", Computing Technology and Information Management (ICCM), 8th International Conference,Vol. 1, pp.141-145