International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST218274

Investigating the Energy Efficient Routing Protocol for Wireless Sensor Networks

Harmanpreet Kaur*[1], Manoj Kumar Srivastava[2]
*[1]M.Tech (Scholar), CSE Depatment Desh Bhagat University, Mandi Gobindgarh, Punjab, India
[2] CSE Department, Desh Bhagat University, Mandi Gobindgarh, Punjab, India

Article Info
Volume 8, Issue 2
Page Number : 422-427

Publication Issue
March-April-2021

Article History
Accepted : 10 April 2021
Published : 18 April 2021

ABSTRACT

A Wireless Sensor Network(WSN) consists of chain of sensors with capabilities of consuming energy for sensing, computing, and wireless communication to track physical device and relay their data to a base station cooperatively via the network. Efficient path for the processing of data in WSN and also to identify the active devices in the path. The ad-hoc networks which are active in WSN due to protocol, they facilitate versatility that often alters the topology. The Energy Efficient Zone based Routing Protocol (ZBEEP) which is the latest protocols in this direction, and the most common is On Demand Distance Vector Ad-hoc routing protocols. In ABODV and ZBEEP protocols using Network Simulator, I simulated this Black Hole Attack and tried that in the case of ZBEEP protocol the effect of energy due to Black Hole Attack is ineffective and better as compared to ABODV. I used two service quality metrics, such as Packet Transmission Ratio and Through-put, to help my opinions.

Keywords : Black Hole Attack, MSN, Protocol, Energy, and ZBEEP.

I. INTRODUCTION

The appearance of mobile computing has revolutionized our info society. The proliferation of new, powerful, and compact act devices, having extraordinary process power sealed the means for advance mobile connectivity. We have a tendency to be moving from the private pc age to the ever present Computing age within which a user utilizes, at a similar time, several electronic platforms through which he will access all the specified information whenever and where needed. The character of ubiquitous devices makes wireless networks the best resolution for his or her interconnection and, as a consequence, the wireless arena has been experiencing exponential growth within the past decade. There are, several things wherever user needed networking connections aren't obtainable in an exceedingly given geographic area, providing the required property and network services in all conditions becomes a true challenge [1]. A Wireless Sensor Network (WSN) is a group of pretty less

expensive computational nodes that degree neighbourhood environmental situations like temperature, sound, strain and many others and ahead such data to a base station for appropriate processing [2]. WSN is by some means much like advert hoc cellular community in the experience that each are useful resource constrained, just like the battery power, capacity, conversation variety and memory. WSNs nodes can experience the environment, can speak with neighbouring nodes, and can, in lots of cases, carry out primary computations at the facts being collected, means Sensor nodes are deployed randomly within the software area, because of that, the WSN has various tiers of node density alongside its area. The likely difference of node density amongst a few areas of the community has the energy constraint of the wireless sensor nodes due to which some nodes degrade making the particular bunch much less dense. Overall it's appealing not unusual to set up WSNs in the Detroit environment, so the many wireless sensors have fault [3]. For which, networks should be fault-tolerant and protection is minimized. Typically conversion is dynamic in topology. The resultant for this trouble is to deploy protocols that carry out efficiently making use of less quantity of energy as viable for the conversation amongst nodes. The Wireless sensor network may be described as a wi-fi sensor network that follow specific path in the network. These sensor nodes may associate to specific moving nodes. Sometimes those nodes need to flow because of the surroundings in which they're associated.

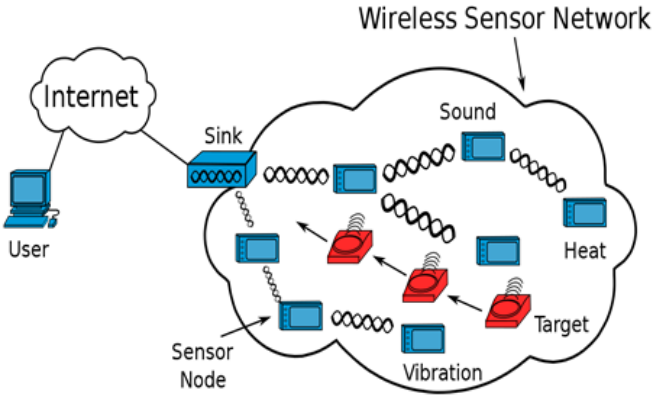

Figure 2: Wireless Sensor Network architecture [14]

II. PROBLEM STATEMENT

Here in paper we try to investigate green power protocol ZBEEP and scrutinize the effects and consequences how black-hole on ZBEEP primarily based on a few arguments. Here in paper different segment specified which can gift to speak approximate running ideas of ZBEEP and approximately the black-hole assault, the way it works. The other segment wills complex our proposed protocol ZBEEP approximately how black-hole reasons hassle for ZBEEP. Next segment analyses the overall performance of current and the use of extraordinary graphs. Last segment describes the belief and destiny paintings observed via way of means of references.

III. RELATED WORK

There are numerous methods supplied via way of means of exceptional authors relating each stable and non-stable routing protocols. Initially, there's numerous literature research targeted on reviewing seek issues on stable routing in WSNs. Subsequently, present research taken into consideration numerous troubles like as electricity efficiency [4], location-primarily based totally [5], Network topology, community scalability and maintainability, powerful records transmission, routing and stable multi-direction routing and security etc. The

importance of the proposed routing protocol is to reap statistics securely and shield the overall performance of the community from degradation and different resources. From this method can shield statistics exchange, stable records transport in addition to replace the rout via way of means of isolation of malicious nodes.

All the ones investigational research offer an in depth look at of various routing schemes. However, this segment is specially specializing in a complete survey look at of stable routing protocols in WSNs. Other proposed a trust-primarily based totally mechanism with stable routing approach for WSNs and explored the contemporary studies look at and become aware of the open studies demanding situations via way of means of surveying proposed mechanisms [6]. Later, they categorized the earlier routing protocols primarily based totally at the form of routing assaults and supplied complete studies on a trust-primarily based totally mechanism to stable the routing in WSNs. They supplied a trust-primarily based totally stable routing mechanism that establishes a honest stable routing among every sensor nodes to the vacation spot node.

Energy green routing protocols sensor nodes store their electricity stage via way of means of the usage of extraordinary strategies to growth node and community lifetime. Introduction of quarter growth the electricity performance as handiest quarter head have the authority to ship and get hold of data. For this facility different member nodes might not energetic all of the time, it saves nodes electricity and growth community lifetime [7]. Energy performance is an essential problem in MSN. The present electricity-green routing protocols often use final electricity, transmission power, c programming language among nodes as metrics to pick out a most advantageous path. Obviously the node with maximum electricity decided on as a quarter head. The intention of ZEEP protocol is to lessen the wide variety of manipulate packets while attempting to find a route [8].

IV. SECURITY ISSUES

A. Active and Passive Attacks: In passive assaults the attacker does now no longer ship any message, however simply listens to the channel. Passive assaults are non disruptive however are records seeking, which can be essential within the operation of a protocol [9]. Adversaries want now no longer be bodily gift to keep surveillance; they are able to accumulate records at low-chance in nameless manner. In a wi-fi surroundings it's miles typically not possible to locate this type of attack, because it does now no longer produce any new trace within the network. Active assaults may also both be directed to disrupt the everyday operation of a specific node or goal the operation of the entire network. The motion of an lively attacker consists of injecting packets to invalid locations into the network, deleting packets, enhancing the contents of packets.

B. Impersonation Attack: With the loss of authentication in ad-hoc networks, IP addresses uniquely discover hosts[10]. Therefore non repudiation is not supplied for ad-hoc community protocols. MAC and IP spoofing are the most effective strategies to faux as some other node or disguise within side the community. Malicious nodes attain impersonation most effective with the aid of using converting the supply IP cope with within side the manipulate message. Another purpose for impersonation is to steer nodes to alternate their routing tables pretending to be a pleasant node, including assaults towards routing table. An example of impersonations, Man-in-the-center assault [11]. Malicious node plays this assault with the aid of using combining spoofing and losing assaults. Physically, it need to be

positioned because the most effective node in the variety for vacation spot, within side the center of the course or sufferer node need to be averted from receiving every other course statistics to the vacation spot. The affected node routing tables can be used to redirect packets, the use of assaults towards the routing table.

C. Gray Hole Attack: Gray hollow assaults is an energetic assault type, which result in losing of messages. Attacking node rest consents to ahead packets after which fails to do so. Initially the node behaves successfully and replays real RREP messages to nodes that provoke RREQ message. This way, it takes over the sending packets. Afterwards, the node simply drops the packets to release a (DoS) denial of carrier assault. If neighboring nodes that try and ship packets over attacking nodes lose the relationship to vacation spot then they'll need to find out a path again, broad-casting RREQ messages.

D. Selective Forwarding Attack: Multi hop networks are primarily based totally at the concept that collaborating nodes will faithfully ahead acquire messages. Malicious nodes may also refuse to ahead positive messages and actually drop them, making sure that they're now no longer propagated any similarly within the network. Selective forwarding assaults are usually maximum effective while the attacker is explicitly blanketed at the route of a statistics [12].

V. BLACK HOLE ATTACK

Black hollow is one sort of protection assault in which a malicious node sends faux routing information, it has a top-quality course in the direction of vacation spot and reasons different proper nodes to course statistics packets via the malicious one. This is a well-known ad-hoc routing assault in which nodes are dropped.

In this assault a malicious node makes use of the ad-hoc routing protocol (right here we use ABODV) to put it up for sale itself as having the shortest course to the node whose packets requires to detain. As ABODV is published primarily based overall protocol, right here if malicious respond reaches to supplicate the node earlier than the response from the actual node, a cast course has been created. This malicious node then can pick whether or not to drop the packets to carry out a denial-of-carrier assault or to apply its region at the course because the rest assault in between[13]. As the example follow, in ABODV, the attacker can ship a faux RREP(together with a faux series quantity which is fabricated to be identical or better than the only contained with inside the RREQ) and reducing hop-matter fee to the supply node, claiming that it has a sufficiently clean course to the vacation spot node. This reasons the supply node to pick out the course that passes through the attacker.

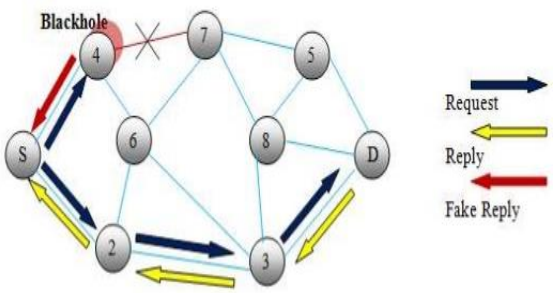

Figure 2: Black hole Attack in protocol [15]

This trouble of complexity made sensor networks extra at risk of the various safety attacks, where in packet drop assault that's pretty not unusual place and dangerous assault that influences the community tier. In dangerous assault the adversary biases the wireless sensor node to drops the whole packets which might be forwarded to it. Here in research, the method to know-how primarily based to gain knowledge of used by detection and easing of these dangerous nodes from the community liable for activating the assault.

VI. ANALYSIS AND RESULTS

The traffic reasserts are CBR (non-stop bit rate). The source-vacation spot pairs are unfold randomly over the community. The mobility version makes use of random waypoint version in a square led of 900m x 900m with 50 nodes. During the simulation, every node begins off evolved its adventure from a random spot to a random selected vacation spot. Once the vacation spot is reached, the node takes a relaxation time period in 2nd and any other random vacation spot is selected after that pause time. This system repeats during the simulation, causing continuous modifications within the topology of the underlying community. Different community state of affairs for different quantity of nodes and pause instances are generated.

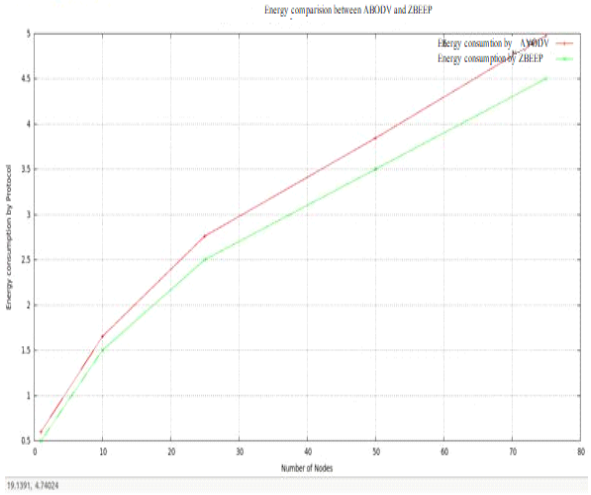

Figure 3: Energy difference of ABODV and ZBEEP

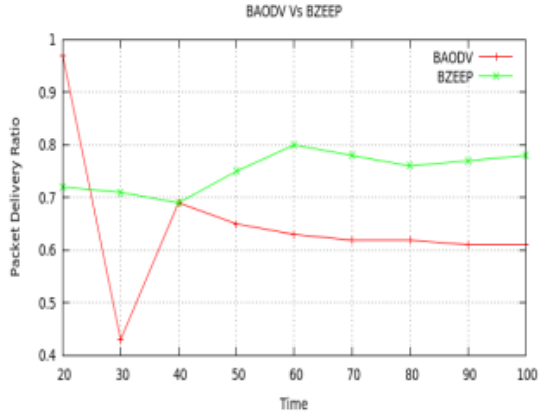

Figure 4: Comparison of BAODV and BZEEP using Packet Delivery Ratio performance

VII. CONCLUSION

These simulation effects have proven that ZBEEP has a higher overall performance in comparison to BAODV protocol consumes less energy of the network. Black hole(dangerous assault) ZBEEP offer higher packet transport ratio along with throughput than black hole(dangerous assault) BAODV. Thus in manner the effect of dangerous assault is extra intense in case of BAODV the energy efficient routing protocols for wireless sensor.

VIII. REFERENCES

[1]. K Sohraby,D Minoli,T Znati, Wireless Sensor Networks , Technology, Protocols, and Applications

[2]. Getsy S Sara and D. Sridharan, Routing in mobile wireless sensor network: a survey, Springer, Aug. 2013.

[3]. Faisal Bashir Hussain, Usama Ahmed, "Energy Efficient Routing Protocol for Zone Based Mobile Sensor Networks ", IEEE 2011, pp.1081-1086.

[4]. A. K. Sadek, W. Su, and K. J. R. Liu, Multi-node cooperative communications in wireless networks, IEEE Trans. Signal Processing, vol. 55, no. 1, pp. 341-355, 2007 .

[5]. Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados , "Energy-E cient Routing Protocols in Wireless Sensor Networks: A Sur-vey" , IEEE Communications Surveys and Tutorials, VOL.15, NO. 2,Second Quarter 2013.

[6]. J R Srivastava, TSB Sudarshan ,ZEEP: Zone based Energy E cient Rout-ing Protocol for Mobile Sensor Networks , IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCl) , 2013 .

[7]. P. Yau and C. J. Mitchell, Security Vulnerabilities in Adhoc Network.

[8]. G. Vigna, S. Gwalani and K. Srinivasan, An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks, Proc. of the 20th Annual Com-puter Security Applications Conference (ACSAC04).

[9]. G. Padmavathi and D. Shanmugapriya A Survey of Attacks, Security Mech-anisms and Challenges in Wireless Sensor Networks.

[10]. B Kannhavong, H Nakayama, Y Nemoto, N Kato, A Jamalipour, A Survey Of Routing Attacks In Mobile Ad hoc Networks , IEEE Wireless Commu-nications.

[11]. Virtual InterNetwork Testbed, http://www.isi.edu/nsnam/vint, The NS Manual.

[12]. http://www.isi.edu/nsnam/ns/doc/nsdoc.pdf .

[13]. http://www.isi.edu/nsnam/ns/.

[14]. https://en.wikipedia.org/wiki/Wireless_sensor_network

[15]. https://ns2code.com/ns2-black-hole-attack

Cite this article as :

Harmanpreet Kaur, Manoj Kumar Srivastava, "Investigating the Energy Efficient Routing Protocol for Wireless Sensor Networks", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 2, pp. 422-427, March-April 2021. Available at
doi : https://doi.org/10.32628/IJSRST218274
Journal URL : https://ijsrst.com/IJSRST218274