World Wide Journal of Multidisciplinary Research and Development

World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(7): 44-47
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Sukhwinder Kaur
M.Tech (I.T.) & Guru Kashi University Talwandi SaboBathinda, India

Lovepreet Kaur
Assistant Professor of GGSCET Guru Kashi University, Talwandi Sabo Bathinda, India

Correspondence:
Sukhwinder Kaur
M.Tech (I.T.) & Guru Kashi University Talwandi Sabo Bathinda, India

Enhanced GA Based Approach to Detect the Energy Draining Nodes in the Wireless Sensor Networks

Sukhwinder Kaur, Lovepreet Kaur

Abstract
Wireless sensor networks are created by nodes which are deployed for specific kind of application. These nodes are tiny sensors and are powered by cells or limited batteries. Since the time these networks came into existence, conserving their energies has remained one of the prime goals of the researchers. Security on the other hand is another issue faced by such networks as these networks are left unattended after being deployed. However, some of the attacks are related to consuming up the energy of the nodes. For example, flooding attacks, vampire attacks etcetera are suck kinds of energy draining attacks. Detection and prevention of such kinds of attacks become extremely important. This paper presents the defense mechanism against one of the energy consuming malicious node which would flood more packets during the time of data communication. The performance of the scheme has been analyzed in terms of throughput, number of packets forwarded and remaining energy in the network. These parameters have shown an improvement.

Keywords: WSN, energy draining attacks, vampire attack, throughput.

Introduction
WSN applications furthermore, correspondence protocols are predominantly custom fitted to give high energy efficiency. Sensor nodes convey constrained power sources. Thusly, while customary systems are intended to enhance execution measurements, for example, throughput, WSN protocols concentrate principally on power preservation. The arrangement of WSNs is another calculate that is viewed as creating WSN protocols. The position of the sensor nodes require not be designed. Due to the short transmission ranges, extensive quantities of sensor nodes are thickly conveyed and neighboring nodes might be near each other. Thus, multi-route correspondence is misused in interchanges between nodes since it prompts to less power consumption than the single route correspondence. Subsequently, the spatio-worldly relationship based protocols developed for enhanced efficiency in systems administration wireless sensors.

Traditional security goals for an ad-hoc network and specific to the WSN security goals can be classifies in two categories as primary and secondary [8]. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, Self-Organization, Time Synchronization and Secure Localization [9].

Since energy conservation is one of the major goals of wireless sensor network, some of the attacks are related to consuming up the energy of the nodes. For example, flooding attacks, vampire attacks etcetera are suck kinds. This paper considers another type of attack in which the malicious node floods more packets during the time of data communication between the nodes. Furthermore, section II shows survey of techniques related to detection and prevention of energy draining attacks. Section III represents the proposed scheme and results have been shown in Section IV of this paper.

Relative Work
P. Rajipriyadharshini et al, [2015] gives an answer for vampire attacks Energy is the one most essential element while considering sensor nodes. Remote sensor networks require answer for saving energy level. Consequently, there is a huge of energy misfortune. New protocol called PLGP, a significant and secure protocol is proposed alongside the key management protocol called Elliptic Diffie-Hellman key trade protocol to keep away from this vampire attack [1].

C Chahana B. Thakur [2015] In this paper talk about two sorts of vampire attack. In which proposed System included a Flag _Field as a security Component to the bundle header to keep away from packets circles or extend attack. This Flag Field is 8 bit in size along these lines does not possess much space in the header.The proposed framework recognizes and dispense with vampire node in versatile specially appointed network which bringing on vampire attack [2].

Kavya. H. B, [2015] Vampire Attacks are unsafe sort of attacks as in most exceedingly awful case a solitary Vampire can bring about a network wide energy by a variable of O (N) where N is the quantity of nodes in the network. In an Ad hoc remote network amid the attacks in packet forwarding the energy utilization is expanded in network. In this paper, the primary highlight of the execution is to forestall foe impact on the nodes battery control and to set up the secured transmission with less energy utilization [3].

Miss. V. Subha [2014] proposed new protocol called VSP, an important and secure protocol alongside the key management protocol to maintain a strategic distance from this vampire attack. By utilizing this, current issues can be overcome. The current framework does not offer a completely palatable answer for Vampire attacks amid the topology revelation phase, yet recommended some instinct about harm impediments conceivable with further changes to PLGPa. [4]

Eugene Y. Vasserman et al [2014] locate that all analyzed protocols are defenseless to Vampire attacks, which are ruinous, hard to distinguish, and are anything but difficult to do utilizing as few as one noxious insider sending as it were protocol-agreeable messages. sCreator talks about strategies to relieve these sorts of attacks, including another confirmation of-idea protocol that provably limits the harm brought on by Vampires amid the packet-forwarding phase [5].

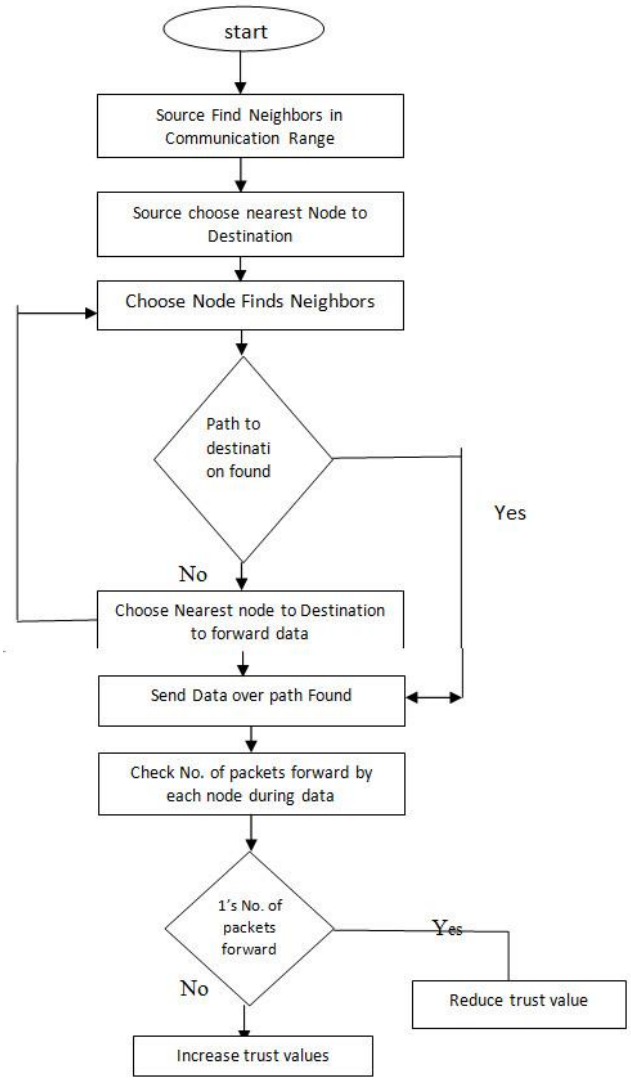
Jose Anand [2014] In this paper, the routing protocol influenced by vampire assault in WSN is examined. This is another class of asset utilization assault that utilization routing protocols to for all time cripple adhoc WSNs by exhausting node's battery control. Reenactment comes about demonstrate that relying upon the area of enemy, network energy consumption amid the forwarding phase expanding. The security defects of AODV can be settled by utilizing RSA encryption framework that will keep away from the enemy from entering the framework [6].

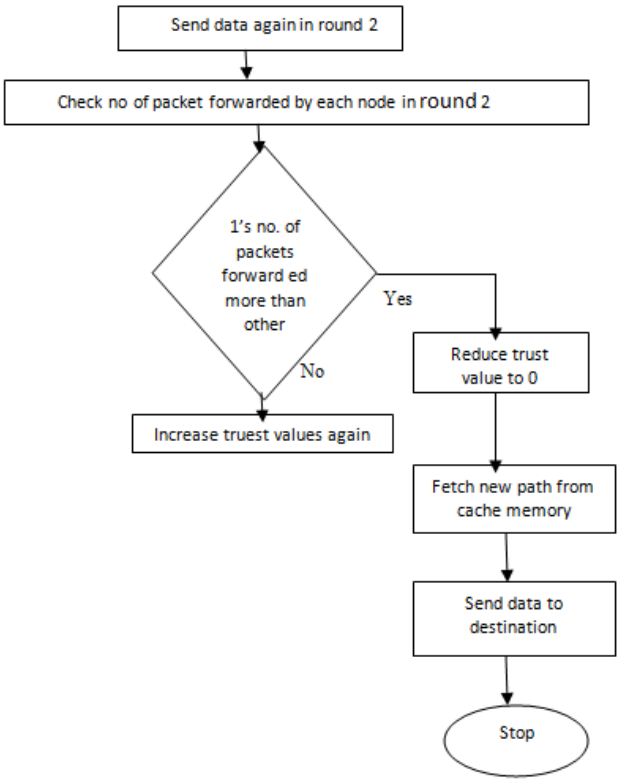
Gurbindersinghbrar et. al.,[2016] proposed PDORP protocol which is transmission-based energy aware routing protocol. The proposed protocol PDORP has the characteristics of both power efficient gathering sensor information system and DSR routing protocols. Hybridization of genetic algorithm and bacterial foraging optimization is connected to proposed routing convention to distinguish energy proficient ideal ways. The execution examination, correlation through a hybridization approach of the proposed routing convention, gives better outcome involving less piece mistake rate, less postponement, less energy utilization, and better throughput, which prompts to better QoS and drag out the lifetime of the system. Besides, the calculation model is adopted to assess and think about the execution of the both routing conventions [7].

Proposed Work

When the source has some data to send to the destination node, the traditional broadcasting process of flooding the RREQ packets will not be followed. This is because lesser batteries drive the sensor nodes, so broadcasting will consume much of their batteries. Therefore, nodes will use the GPS routing, in which the source node will first look for the neighbors in the communication range.From all these neighbors, the two nodes will be selected that will be closest to the destination node.

Once the path is formed from source to destination, the source node would begin data transmission over the path formed. At the end of the data transmission, the trust values of the nodes would be computed according to the behavior of the nodes during the data transmission process.If any node has went on to flood the packets, then its trust value would be reduced. Reduction of trust value would help to detect the malicious node, which would be eventually removed from taking part in further communication.





Results

The performance of the network was analyzed based on three parameters namely remaining energy, throughput and number of packets forwarded in the network.

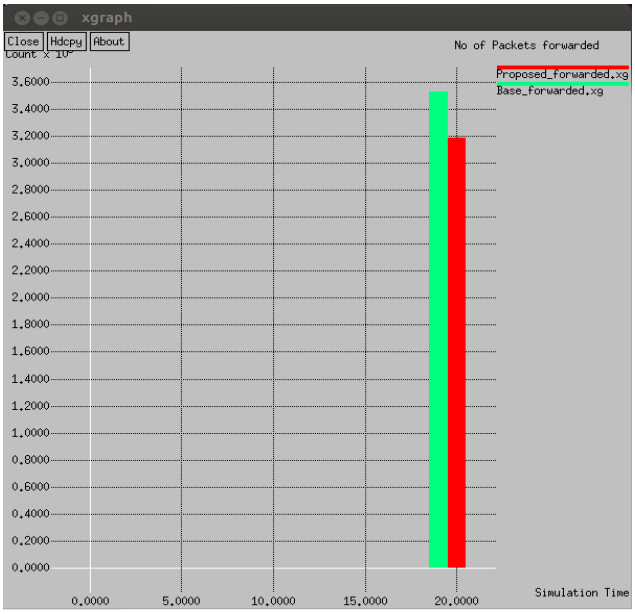


Fig. 1: Comparison of Number of Packets Forwarded

The figure shows the number of packets forwarded by the nodes in both the schemes. The value is more for the existing scheme (approx. 3590) and less for the proposed scheme (approx. 3190).

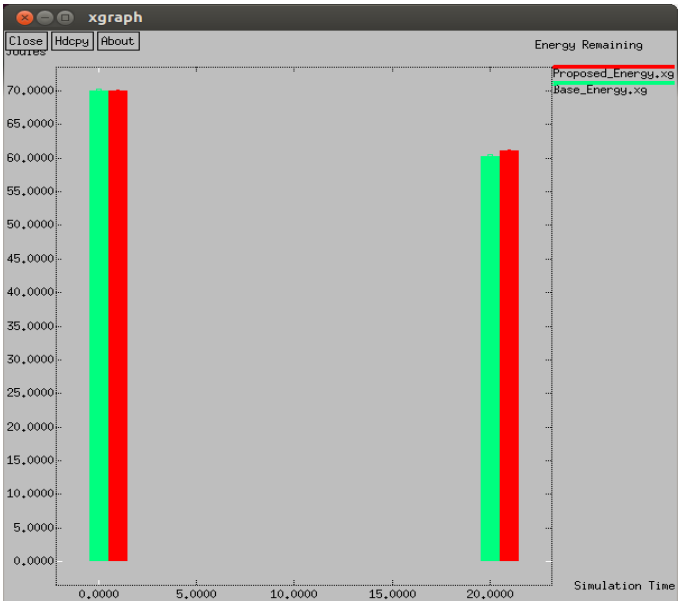


Fig. 2: Remaining Energy comparison

This shows that remaining energy for the proposed scheme is more than the existing scheme. Since number of packets forwarded are more in the existing scheme so it becomes evident, that attacker node has used more energy of the nodes leading to lesser remaining energy.

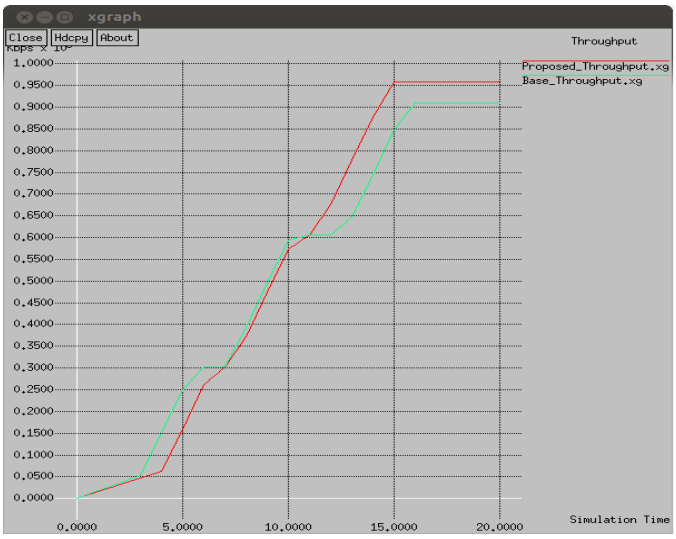


Fig. 3: Throughput Comparison

This figure shows the amount of data received at the destination node, i.e. throughput. Since the more forwarding of the packets leads to congestion over the links.Therefore, packets start getting dropped leading to lesser throughput. The value of the throughput for the proposed scheme is 952 Kbps and for the existing scheme, the value was 910 Kbps.

	Remaining Energy	No. of packets Forward	Throughput
Base	60.1734	3527	909 kbps
Proposed	61.0656	3181	958 kbps

Conclusion

The energy remaining of the network after the application of the proposed scheme was more as compared to the existing scheme. In addition, number of packets forwarded

were less for the proposed scheme. When the malicious node forwards more number of packets, its energy is bound to go down. Nevertheless, the malicious node can forward more packets in a way that its energy does not goes down to a level, which makes it possible to detect the attacker. Therefore, in every round, the malicious node can forward more number of packets without being detected in the network. This also leads to more energy consumed for the existing scheme and less for the proposed scheme. Thus, it can be concluded that proposed scheme has outperformed the existing scheme.

In future, the proposed scheme can also be used to detect the hello flood attack in the clustered wireless sensor networks because in the hello flood attacks also, the attacker node forwards more hello packets to form larger clusters.

References

1. P.Rajipriyadharshini,. Venkatakrishnan, S.Suganya, A.Masanam "Vampire Attacks Deploying Resources in Wireless Sensor Networks" Department of Computer and Software Engineering Feb 2015.
2. C Chahana B. Thakur, V.B. Vaghela "Detection and Elimination of Vampire Attack in Mobile Ad hoc Network", in International Journal of Computer Science and Mobile Computing Volume - 5 Jan– 2015.
3. Kavya.H.B, Manjunath R Raikar "Prevention of Vampire Attacks to Control Routing Behavior in Wireless AD Hoc Networks" International Journal of Computer Science and Mobile Computing in July 2015.
4. Miss. V.Subha, Mrs. P.Selvi, " Defending against vampire attacks in wireless sensor networks" in International Journal of Computer Science and Mobile Computing, Vol.3 Issue.11, November- 2014.
5. Eugene Y. Vasserman and Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE Transactions on mobile computing, Vol. 12, No. 2, February 2013
6. Jose Anand , K. Sivachandar, " Vampire Attack Detection in Wireless Sensor Network" in International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 4, July 2014.
7. Gurbindersinghbrar, Shalli Rani, Vinay Chopra, Rahul Malhotra, "Energy Efficient Direction-Based PDORP Routing Protocol for WSN" in IEEE 2016.
8. Vikash Kumar, Anshu Jain and P N Barwal, "Wireless Sensor Networks: Security issues Challenges and Solutions" in International Journal of Research in Engineering and Technology, November 2014.
9. Vishal Rathod, Mrudang Mehta, " Security in Wireless Sensor Network: A survey" in Ganpat university journal of engineering & technology, 2011.