International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 5 Issue: 5
ISSN: 2454-4248
10 – 12

A Proposal towards Detection of Sybil Attack Using Sink Based Detection Mechanism in Wireless Sensor Networks

Pushpinder Kaur[a], Anil Jaswal[b]
a Research Scholar, Global College of Engineering and Technology, Amritsar, Punjab, India
[a]ghumanpushpinder@gmail.com
[b] Global College of Engineering and Technology, Amritsarr, Punjab, India

Abstract: Recent advances in wireless and electronic communications have enabled the deployment of low-cost, low-cost, low-power, multi-function sensors and communicate in a nutshell. Intelligent and economical sensors, connected to the network via wireless links and distributed in large quantities, offer unprecedented opportunities to monitor and control homes, cities and the environment. In addition, sensors connected to the network use a wide range of applications within the defence area, generating new features for recognition and surveillance and various tactical applications. Sybil is one of the most terrible attacks is the cloning attack of the node, where the attacker captures the knot and extracts its secret information, create replicas and enter them in the network field other malevolent behaviour. In this paper, to detect and mitigate this attack, sink-based detection schemes have been proposed.

*****

I. Introduction

A Wireless device Network (WSN) is formed by many tiny, cheap low memory nodes and less energy, and process capability. In Such specific variety of WSNs, many issues arise to find out every node. Current advancements in wireless transmissions have facilitated to roll-out the cheap, less energy and versatile sensors that are tiny in size and transmit in a miniature distance. Inexpensive and good sensors are associated with the help of wireless channels and positioned in large amount. Moreover, the sensors which are associated or networked use a wide range of applications between the defense area, creating novel potential for intelligence and police work and numerous military science fields. Self-relocation capabilities are often an extremely fascinating sign of wireless device networks. The examples of environmental based applications are water quality checking and agriculture; the measuring data are not at all meaningful. Moreover, location estimation might alter several applications as an example of Intrusion Recognition, Stock Organization, Traffic Monitoring, Health Examination, intelligence and police work.

With all the development inside the reduction and incorporation of the finding and transmission technologies, the system of high level wireless mechanisms uses a considerable amount of economic sensors and low energy consumption previously realized. Within a wireless device system, the nodes of the powered devices are scattered in a physical space. Each device within the sensor network collects information, for example, detection of vibrations, temperature, radiation and various environmental factors.

II. Related Work

R. Upadhyay et.al. [1] Said that WSNs is a financial as well as problem free answer for a diversity of applications. The open character of wireless sensor networks makes it incapable against a range of security threats. A variety of security attacks like wormhole attack, black hole, distributed denial of service attack. It is likely to work together with the information as well as the sensor node in the network. In this manner, the drainage of the power of the battery unswervingly debases the existence of the node. Moreover, this work considered it a solemn dilemma and planned a resolution to conquer the trouble of power consumption owing to distributed denial of service attack.

S.Maidhili R et.al.[2] Said that WSNs are likely to be vulnerable when they select the cluster head between sensor nodes. IDS cannot avoid it or act, but it can only detect it. IDS informs the controller to take the necessary measures when activating the alarms if an attack is detected, which is positive, but also involves a waste of resources and a waste of time in the detection process. Prevention must be carried out in the state of launch of the attack so as to minimize the waste of resources and the consumption of time. Initially, the attacker launches the attack to enter the selection of group heads (CH) that transmit control messages with false information, such as high energy & neighbour counting. The results of the experimental simulation work, to detect attacks at the basic level & improve network performance, to avoid the attack in order to reduce the resource overload and to perform routing & aggregation of data resident in the WSN.

O,Can et.al. [3] Proposed that the WSNs is a large-scale network with dozens of hundreds of small devices. The use of WSN fields such as the army, health, the smart home has a large scale and its areas of use are increasing day by day. The WSN safe theme is an important research area & WSN applications have some important security shortcomings. The intrusion detection system is a second line of network security mechanism and is very important for integrity,

 ISSN: 2454-4248
10 – 12

privacy and availability. Intrusion detection in WSN is something other than wireless networking with no power restrictions, since WSN has some restrictions that affect the types of attacks and cyber security attacks. This paper is a survey that describes the types of attack of WSN intrusion detection approaches that oppose this type of attack.

S. Rao et. al.[4] Studied and analyzed the impact of the jam on micaz specks running Tiny OS and explores ways to mitigate the impact. Interference is facilitated by disabling the detection of the carrier on the interference nodes. The interference attack is detected while monitoring RSSI and PDR on the receiver. Varying different parameters in the sender, such as power level, package size, distance with theoretical analysis

S. Nagar et.al.[5] Introduced a secure protocol for WSNs, which is capable of overcoming the distributed denial of service attack in the network. In our proposed approach analysis is done on the malicious nodes by means of the methodology and obstructs that node from any other movement in the network. Therefore, in order to defend the network, authors make use of an intrusion prevention scheme in which particular network nodes perform as an intrusion prevention node. Moreover, such nodes run in their radio series for the area of the network and frequently examine nearby nodes. At last, when the intrusion prevention node come across a misbehavior node which engage regular distribution messages apart from user datagram protocol and transmission control messages, the intrusion prevention node lumps the malicious node as well as transmits the information to every original dispatcher nodes to amend its routes.

T.Kaur et. al.[6] Said that with the advancement and innovation, one of the fundamental concerns nowadays is security. There are a few conceivable assaults on WSN, in DDOS assaults (Distributed Denial of Service), malignant nodes are adjusted to numerous assaults, for example, flood assaults, dark gaps and hot-opening assaults, to stop the general activity of the system. The dangers are considerably more prominent when one talk about military and modern applications. Besides, there are numerous confinements in WSN, for example, constrained battery limit, low bunch limit, and so forth. Showing a security demonstrates that thinks about these confinements and gives security is a noteworthy test nowadays. There are a few instruments proposed by scientists to recognize or shield against this DDOS assault.

P. Gosavi et. al.[7] Said that specially appointed wireless systems are dynamic in nature. Ad-Hoc systems don't rely upon any default foundation. At whatever point correspondence is required by then, this system can be executed. In this article they talk about vampire assaults. Vampire assaults are anything but difficult to perform through the system and hard to distinguish. At that point they contrast the new technique and the current convention and Beacon Vector directing. What's more, they reach the resolution that the new convention is better, since it distinguishes and anticipates vampire assaults.

III. Proposed Approach

There are many techniques which different researchers have proposed in order to attack dos attacks but the major limitation of them is the congestion among those nodes. Due to congestion, the drainage of battery becomes fast and nodes become dead rapidly. So, in this research work, we will distribute the traffic among gateway nodes so as to minimize the traffic load and to enhance the battery depletion problem. Therefore as per the literature survey conducted, the problem is the traffic among every node as every node becomes busy in detection DOS attack.

Thus following proposed methodology will help to mitigate this problem of sybil attack.

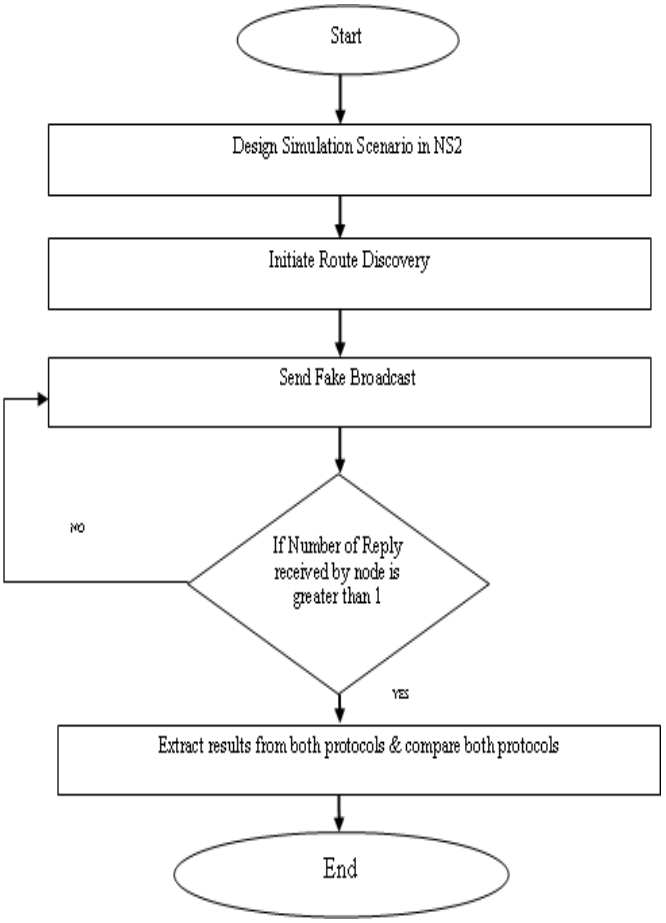

Figure 1: Proposed Methodology

IV. Conclusion

One of the most alarming attacks in the WSN is the cloning attack of the nodes where the attacker takes the details of the node and collects their personal data, duplicates them and inserts them into the network field for further malicious activities. To detect and eliminate this type of attack, different detection

 ISSN: 2454-4248
10 – 12

techniques have been designed based on both static and mobile WSNs.

This paper proposed the methodology overcome Sybil attack in a proficient way.

References

[1] R.Upadhyay, S. Khan, H. Tripathi, U. Rathore Bhatt, "Detection and Prevention of DDOS Attack in WSN for AODV and DSR using Battery Drain," Intl. Conference on Computing and Network Communications (CoCoNet'15), 2015.

[2] S.Maidhili R, Karthik GM, "Intrusion Detection and Prevention Based on State Context and Hierarchical Trust in WSNs," International Conference on Computer Communication and Informatics, Coimbatore, INDIA, 2018.

[3] O. Can and O. Sahingoz, "A Survey of Intrusion Detection Systems in WSNs," IEEE, 2015.

[4] S. Rao, Deepak S and P. Pradeep, "Parametric Analysis of Impact of Jamming in WSNs," IEEE, 2013.

[5] S.Nagar, S.S Rajput, A.K Gupta and M.C Trivedi, "Secure Routing Against DDoS Attack in WSNs," 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT), 2017.

[6] T. Kaur , K. Saluja and A. Sharma, " DDOS Attack in WSN: A Survey," IEEE International Conference on Recent Advances and Innovations in Engineering, Jaipur, India, 2016.

[7] P.. Gosavi and B. Patil, "Draining Life from Wireless Ad – hoc Sensor Networks," International Journal of Computer Applications (0975 – 8887) Volume 144 – No.9, June 2016.