Review on Network Monitoring and Trust Routing in Presence of Dos Attack

Chinmay Kulkarni[1], **Dr D. N. Patil**[2]
[1, 2] Department of Computer Engineering
[1, 2] Sinhgad College of engineering, Pune

Abstract*-In a Wireless Sensor Network (WSN), providing security is one the main issues because of its dynamic topology, wireless network which is open, intermittent connectivity, absence of centralized infrastructure and resource constrained sensor nodes. WSN can be hacked due to these downfalls and can create very dangerous results. Black Hole can be one of them in which it gets a trust of network by showing that the data packet routing to the destination node exploiting that it has a shortest path but in real it drops all packets consequently threatens reliability of network. This survey present some previous work done related to above problem.*

Keywords*-*Attack detection and prevention, Black hole attack, Dos attack.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are becoming more popular invention due to their huge range of use in industrial, environmental monitoring, military and civilian domains. Nodes commonly are simple and low cost because of economic considerations. Many times they are neglected that why they have to face to various kinds of new attacks. A black hole attack (BLA) is amongst the basic attacks and its flow can be described as: attacker gets control of node and drops all packets which are routed via attacked node, as a result very important data will be dropped or are not able to send it to the sink. Due to the network is responsible for making decisions based on the nodes a sensed data, the downfall is that the network will totally fail as well as more seriously can take wrong decisions. That’s why detecting and avoiding BLA is major significance for security in WSNs.

A wireless sensor network (WSN) is a network created by countless sensor nodes where every node is outfitted with a sensor to identify physical concept, for example, light, heat, pressure, etc. WSNs are viewed as a progressive data collection strategy to developed the data and communication system which will enormously enhance the dependability and effectiveness of infrastructure frameworks. Contrasted and the wired solution, WSNs include less simple deployment and better flexibility of devices. With the fast innovative improvement of sensors, WSNs will turn into the key technology for IoT.

The security in wireless sensor networks (WSNs) is a important issue because of the inherent confinements of computational limit and power use. While an many of security strategies are being created and a various research is going ahead in security field at an brisk pace yet the field does not have a common integrated platform which gives an extensive correlation of the seemingly unconnected yet linked issue user we endeavor to relatively break down the different accessible security approaches highlighting their points of advantages and weaknesses. Numerous sensor network routing protocols have been proposed, however none of them have been composed with security as an objective and propose security objectives for routing in sensor networks.

There are several possible attacks on WNS networks such as black hole attack, DoS attack etc. Black hole attack is occurs, when an intermediary captures and re-programs a set of nodes in the network to block/drop the packets and generates false messages instead of forwarding correct/true information towards the base station in wireless sensor network. There are several technique used to detect black hole attacks in MANET this technique not applied for WSN because of the high computation and storage requirements. A black hole attack is one attack that is fixed by an eavesdropper/adversary on a subsection of the sensor nodes in the network. The eavesdropper/adversary captures these nodes and re-programs them so that they do not pass on any data packets, such as namely those packets they generate and the packets from other sensor nodes that they are supposed to forward.

A Denial of service attack is an explicit attempt to prevent the legitimate user of a service or data. The common method of attack involves overloading the target system with requests, such that it cannot respond to legitimate traffic. As a result, it makes the system or service unavailable for the user. The basic types of attack are: consumption of bandwidth or consumption of processor time, obstructing the communication between two machines, disruption of service to a specific system or person, disruption of routing information, disruption of physical components etc. If the sensor network encounters DoS attacks, the attack gradually reduces the functionality as well as the overall performance of the wireless sensor network. Projected use of sensor networks in sensitive and critical applications makes the prospect of DoS attacks even more alarming.

In this survey, Section II gives the Literature review for Network Monitoring and Trust Routing systems and also list there pros and cons.

II. LITERATURE REVIEW

Wireless sensor networks (WSNs) are progressively being conveyed in security-critical applications. As a result of their inherent resource-constrained, they are inclined to different security attacks, and a black hole attack is a kind of attack that genuinely influences information gathering. To solve this issue an active detection based security as well as trust routing scheme known as Active Trust is developed [1] for WSNs. The most essential advancement of Active Trust is that it avoids black holes through the active creation of detection routes courses to rapidly detect and obtain nodal trust and subsequently enhance the information route security.

This paper [2] proposes a multi-grained block management strategy to improve the space utilization of file systems over PCM-based storage systems. By using the byte addressability and fast read/compose highlight of PCM, a system is designed to dynamically allot multiple sizes of block to fit the size of every document, in order to determine the space fragmentation issue with minimized space and management overheads. The space use of document frameworks is analyzed with thought of block sizes. A series of tests was led to assess the adequacy of the proposed technique, and the outcomes demonstrate that the proposed procedure can essentially enhance the space usage of file systems.

This paper [3] analyses online video replication as well as placement issues in CDNs. A effective video provisioning system should at the same time use framework resources to decrease total energy utilization and limit replication overhead. Author's develops propose a scheme called adaptive data placement (ADP) that can dynamically place and reorganize video replicas among cache servers on subscribers' arrival and departure. Both the analyses and simulation results show that ADP can reduce the number of activated cache servers with limited replication overhead. In addition, ADPˆas performance is approximate to the optimal solution.

In the issue of directing in multi-hop wireless networks, to accomplish top of the end-to-end throughput, it is critical to locate the "best" way from the source hub to the destination node. In spite of the fact that an extensive number of routing protocols have been proposed to discover the path with least total transmission count/time for conveying a single packet, such transmission count/time minimizing protocols can't be ensured to accomplish maximum end-to-end throughput. In this paper [4], Meng et al. argue that by carefully considering spatial reusability of the wireless communication media, they can tremendously improve the end-to-end throughput in multi-hop wireless networks. To bolster their argument, they propose spatial reusability-aware single-path routing (SASR) and any path routing (SAAR) protocols, and contrast them and existing single-path routing and any path routing protocols, individually.

This paper [5] developed the position-aware, secure, as well as efficient mesh routing approach (PASER). Their proposition avoids a greater number of assaults than the IEEE 802.11s/i security mechanisms and the notable, secure routing protocol ARAN, without making restrictive assumptions. In realistic UAV-WMN situations, PASER accomplishes similar performance results as the well-established, non-secure routing protocol HWMP combined with the IEEE 802.11s security mechanisms.

In this paper [6], Ren et al. propose an analytic model to assess the whole system lifetime from system initialization until it is totally disabled, and decide the limit of energy hole in a data-gathering WSN. In particular, they hypothetically estimate the traffic load, energy consumption, and lifetime of sensor nodes amid the whole system lifetime. Moreover, they explore the temporal and spatial evolution of energy hole and apply their analytical outcomes to WSN routing for to adjust the energy utilization and enhance the system lifetime.

In a heterogeneous environment, naive lifetime improvement with participation may not be reasonable. In this paper [7], Kinoshita et al. designed a reasonable cooperative routing technique for heterogeneous overlapped WSNs. It acquaints a energy pool with keep up the total amount of energy consumption by cooperative forwarding. The energy pool assumes a part of agent for fair cooperation.

As shown in table 1, literature review of various papers has been listed, giving possibility of research gap.

Table 1. Survey Table

Sr no.	**Title**	**Publication / year**	**Techniques**	**Advantages**	**Research gap**
1.	ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks	IEEE, 2016	Active Trust	improves both the energy efficiency and the network security performance	---
2.	Multi-Grained Block Management to Enhance the SpaceUtilization of File Systems on PCM Storages	IEEE, 2016	byte-addressability and fast read/write feature of PCM	improve the space utilization of file systems	Supports only one file system
3.	Resource-Saving File Management Scheme for Online Video Provisioning on Content Delivery Networks	IEEE, 2016	ARRIVE and DEPART	reduce the number of activated cache servers	limited replication overhead
4.	SpatialReusability-Aware Routing in Multi-Hop Wireless Networks	IEEE, 2016	Routing Metrics	more significant end-to-end throughput gains under higher data rates	Poor performance
5.	PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks	IEEE, 2016	secure routing protocol ARAN	prevents more attacks than the IEEE 802.11s/i security mechanisms	---

III. PROPOSED SYSTEM

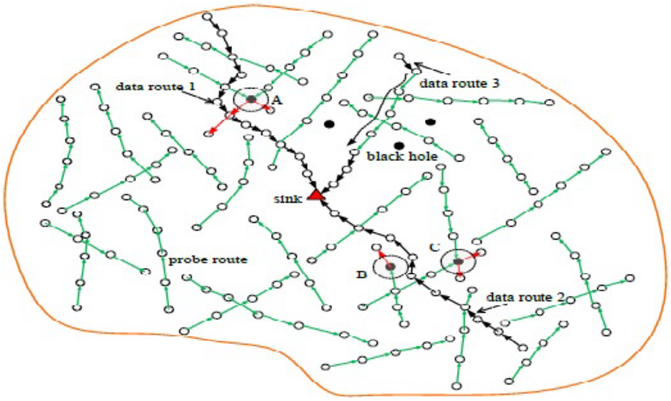

Fig 1. System Architecture

Figure 1 shows the system architecture of proposed system. In proposed system source and destination are selecting and the multiple paths for data transfer are computed. Data will be sending to all computed paths on the network. Data will have detection packet which has the node count between the paths. At every node the value of detection packet is reduced by one and packet is send to next node. If in between the black hole is detected then it can be identified using the value of detection packet.

IV.CONCLUSION

This paper analyses various techniques used for Network Monitoring And Trust Routing. Also given the advantages and drawbacks present in the different studies performed by various researchers. To deal with drawbacks in present systems we presented an idea of the new system.

REFERENCES

[1] Yuxin Liu, Mianxiong Dong, Kaoru Ota, Anfeng Liu, “ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks”, IEEE Transactions on InformationForensics and Security, 1556-6013 (c) 2016.

[2] Tseng-Yi Chen, Yuan-Hao Chang, Ming-Chang Yang, Yun-Jhu Chen, Hsin-Wen Wei, andWei-Kuan Shih, “Multi-Grained Block Management to Enhance the Space Utilization of File Systems on PCM Storages”, IEEE Transactions on Computers, Vol. 65, No. 6, June 2016.

[3] Wen-Hsing Kuo and Yung-Hsuan Lin, “Resource-Saving File Management Scheme for Online Video Provisioning on Content Delivery Networks”, IEEE Transactions on Computers, Vol. 65, No. 6, June 2016.

[4] Tong Meng, FanWu, Zheng Yang, Guihai Chen and Athanasios V. Vasilakos, “Spatial Reusability-Aware

Routing in Multi-Hop Wireless Networks", IEEE Transactions on Computers, Vol. 65, No. 6, January 2016.

[5] Mohamad Sbeiti, Niklas Goddemeier, Daniel Behnke and Christian Wietfeld, "PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks", IEEE Transactions on Wireless Communications, Vol. 15, No. 3, March 2016.

[6] Ju Ren, Yaoxue Zhang, Kuan Zhang, Anfeng Liu, Jianer Chen, and Xuemin (Sherman) Shen, "Lifetime and Energy Hole Evolution Analysis in Data-GatheringWireless Sensor Networks", IEEE Transactions on Industrial Informatics, Vol. 12, No. 2,April 2016.

[7] Kazuhiko Kinoshita, Natsuki Inoue, Yosuke Tanigawa, Hideki Tode and Takashi Watanabe, "Fair Routing for Overlapped Cooperative Heterogeneous Wireless Sensor Networks", IEEE Sensors Journal, Vol. 16, No. 10, May 15, 2016.