Volume: 3 Issue: V Month of publication: May 2015

DOI:

www.ijraset.com
IC Value: 13.98

Volume 3 Issue V, May 2015
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A DBS Intrusion Detection and Prevention System in Wireless Sensor Network

Amanpreet Singh Dehal
Student- Department of Information Technology,
Lovely Professional University, Phagwara, Punjab, India

Abstract— As in the modern era the use of sensor network starts yielding a great importance in variety of applications. Thus certain research work is carried out in this particular field. The thesis will concentrates on how to conserve energy while transferring the data from sender towards receiver in a most efficient way so that the network lifetime is enhanced. Wireless sensor Networks term is refers to a kind of networking that do not requires cables to connect with devices during communication. The transmission is take place with the help of radio waves at physical level. The work would be carried out in network layer through the mechanism of routing. Networking is used to share information like data communication. A network can be wired network and wireless network. Wired network is that which used wires for communicate with each other's and wireless network is that which communicate without the use of wires through a medium. WSN Networks term is refers to a kind of networking that do not requires cables to connect with devices during communication. The transmission is take place with the help of radio waves at physical level. In the WSN sensor study the different characteristics of quality of water, temperature, density, salinity, acidity, chemical conductivity, hydrogen, dissolve methane gas and turbidity. In this work, we are going to prevent the Distributed Denial of Service, Black Hole, Sybil attacks. With this prevention we can enhance the lifetime and performance of network.

Keywords— WSN, Black Hole Attack, DBS, DDOS, Attack Sybil Attack

I. INTRODUCTION

Wireless Sensor Network are emerging as an interesting and promising area. Wireless Sensor Network be fabricated of very large number of heterogeneous/homogeneous nodes. These nodes are interconnects through wireless medium and works cooperatively to sense or monitor the surroundings. The sensor nodes in a network can vary from hundreds to thousands nodes. The nodes senses the environment and forward these information to the sink node through connected neighbours node. The sink node forward this information further to Base station. Mostly network is built only for a single application purpose. Typically WSN are used for disaster monitoring, military surveillance, Industry leakage monitoring, Health care monitoring, pollution monitoring, waste water monitoring and machine health monitoring. Since its type of applications WSN is mostly deployed in hostile environment where it is unattended. In the architecture, each sensor node consist of a radio having transceiver for communication, micro controller for processing abilities, a sensor for sensing or monitoring and battery for providing energy (Ahamed 2009).

The features of sensor nodes are

A. Resource Constraint
B. Unknown topology before deployment
C. Unprotected and Unattended once deployed
D. Unreliable wireless communication

Sensor network is infrastructure of sensing, compute and provide communication between the networking elements. Sensor network heterogeneous network self-possessed of large number of little devices known as nodes. Those nodes are forward information to Base station. A sensor network is a deployment very large numbers of little and self-organized devices that can sense, process and forward to further nodes and able to take the proper actions or decisions for that particular environment. A sensor node is detect state of a certain area like heat, motion, pressure, vibration and sound. The collected information are then forwarded to the Base station that will further processing. Wireless Sensor Network (WSN) applications are suite with IEEE 802.15.4 standards. IEEE 802.15.4 standard is for low rate Wireless Personal Area Network (WPAN) and the standard was defined for wireless Medium Access Control layer and the Physical layer (Sohraby 2007).

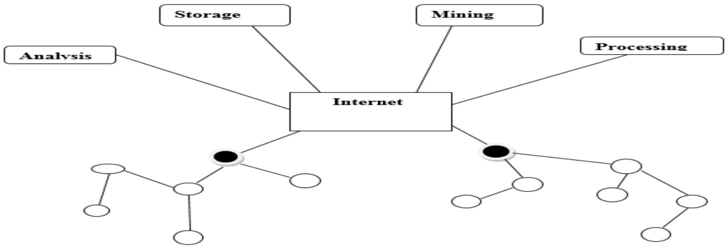


Figure 1: Wireless Sensor Network

II. SYBIL ATTACK

In a Sybil attack the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically.

III. BLACK HOLE ATTACK

Black hole attack is one of most frequent attack that happened in the network. In black hole attack the malicious node falsely advertise that it has the shortest path to the destination. The reason behind such malicious activity is to stop the destination from receiving the packets. In Black hole attacker introduced itself as the destination or it has the shortest path to the destination by replying with a high sequence number RREP message. The source node selects the high sequence RREP message and ignores all other RREP message including the correct ones and starts transmitting the data packets to the malicious node. The malicious node will not forward any data packet to other nodes instead it will drop all the data packets. This type of attack is very severe to detect and we proposed a technique to detect black hole attack.

IV. DDOS ATTACK

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down.

V. LITERATURE REVIEW

Priyanka et.al (2013),"Cluster Based Efficient Caching Technique for Wireless Sensor Networks" In this paper they establish the method or technique in which Global Cooperative Caching for Sensor Networks is used to improve the Wireless Sensor Network working and consistency. Global Cooperative Caching undertakings association among sensor network's judgement for information objects are depend. Grid based technology is used to improve the battery power and its lifetime. After that this method is added increasing to progress for the network performance. (Sharma 2013)

Pathania, Shruti et.al (2010), "Energy Efficient Mechanism to Enhance the Life Time of Wireless Sensor Network" have discussed about metrological approach with different types of magnitudes of parameters like temperature, humidity and discussed all the conditions to trace the weather conditions. A radiation shield is also developed to study the influence of climate and develop a temperature correction model. Classes of data will be defined on the basis of instruments calibration procedures, method, frequency, traceability chain etc. (Pathania n.d.)

Selcuk Okdem et.al (2009)," Routing in WSNs Using an Ant Colony Optimization (ACO) Router Chip" has explained about the stable nodes. Ant colony optimization is based on swarm intelligence. A novel Routing technique using Ant colony optimization algorithm is proposed in the WSNs. Comparative and descriptive study is also mentioned in this paper. It is also implemented on small size component. Adaptive method is established with the help to the objective, their main aim was to maintain maximum life time and so that data receive become efficient. The proposed ACO approach for routing and its implementations is the solutions for node designer. (Okdem 2009)

Xu, Li et.al (2010),” Sink Mobility in Wireless Sensor Networks” In this proposed paper we know about the collected data from the nodes for analysing and uses of it. They explained the balancing of the load battery depletions and movement of the sink node. They deliberated the computation power of sink node and performance of the whole Wireless Sensor Network. They deliberated about the most coming problems in WSN and sing node and give the overview of the models and assumptions. (Li 2010)

Diamond et.al (2007),” Application of wireless sensor network to military information integration” has presented different types of applications in the field of WSN. WSN is used in military applications, health applications, home appliances, environment applications. All these applications have the different impact on each field. The features of these applications are depends on how and where we use or implement wireless sensor network. According to the applications the sensed information and processing on it changes. (Diamond 2007)

Karlof, Chris and David Wagner (2003), "Secure routing in wireless sensor networks: Attacks and countermeasures." In this paper, the technology advances in Micro-Electro- Mechanical Systems which has assisted the development of sensors, we have seen that in very few last years the development and deployment of WSNs in military, environment, surveillance, natural disaster relief, healthcare. These WSNs carry the promise of drastically improving and expanding the quality of services across a wide variety of settings and for different segments of the population. The sensor node provide authentication using Zero Knowledge Proof (ZKP) to add new node in the network then add that node in the cluster. The cluster head selected on the basis on the strong parameters like connect up time, bandwidth performance and battery lift of all the neighbouring nodes. (Karlof 2003)

VI. PROPOSED METHODOLOGY

Security in a WSN is a big challenge because of the large number of nodes and self-configure propriety of network. As we know that security is a major issue in WSN because data is continually transmitting through sensor nodes. The attacks which may be possible on Wireless Sensor Network are:

A. Distributed Denial of Service (DDoS) Attacks
B. Black Hole attack
C. Selective Forwarding attack
D. Eavesdropping attack
E. Wormhole attack
F. Sybil attack
G. Traffic analysis Attack

So here to prevent some of above attacks we are going to propose a new schema which is based on Diffie-Hellman authentication and some parameter based intrusion detection. These parameters are packet received, packet forward and power.

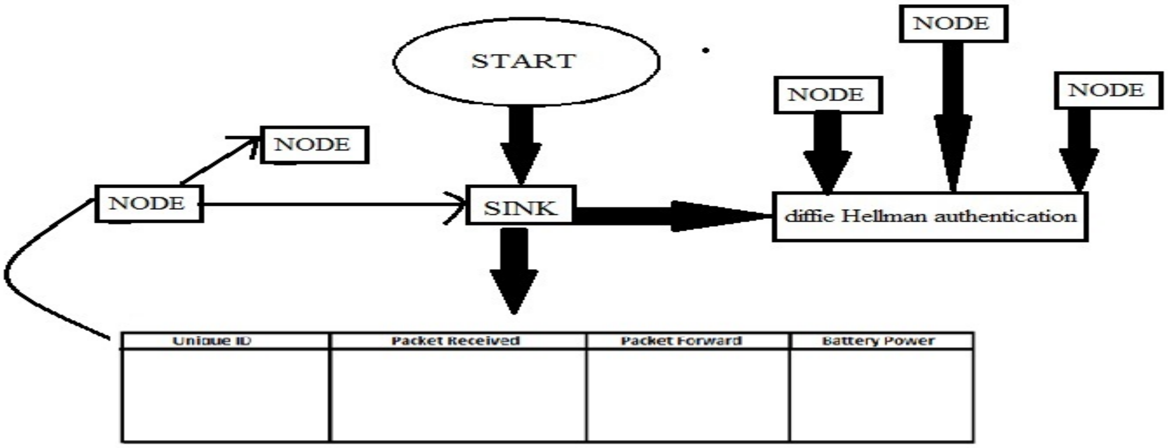
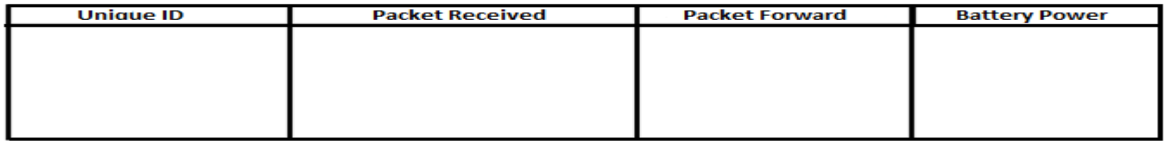


Figure 2: Flow chart

Here sink node will connected to base station. When a new node wants to communicate with the network it will pass through certain steps. New node will be authenticated by the Base station, Base station give a challenge Response Task (CRT) to new node. Now new node will use Diffie-Hellman and give proof of its authentication. Base station will verify the new node and after verification it will assigned unique ID to it if node will authorized, Therefore it will provide the solution of the Sybil attack.

Now to detect DDoS attack on each node is done through neighbour node. The neighbour node collect packet received and packet forward and battery power or lifetime information and send it to base station after the specific time interval. If the difference between the packets received value and packets forward value will very less thus our network working properly or that node not a malicious node, but the difference between these values is large then the Base station check the last three values of these parameters on same node. If the difference is large as this value BS will understand that this node is malicious node and will isolate or block that malicious node.

But if the value of packet forward will zero from last three time intervals, the BS will understand that the node is Black-Hole node and will isolate or block that malicious node.



Unique ID	Packet Received	Packet Forward	Battery Power

Figure 3: Detection table

Now base station will contain this table for each node and on the bases of this table it will take decision about the node.

A. Diffie Hellman Algorithm

1) Base station and all nodes already known the base g = 5 and prime number value p = 23.

2) Base station choose a secret integer a=6 and sends the value of A to node

$A = g^a \bmod p$

$A = 5^6 \bmod 23$

$A = 15{,}625 \bmod 23$

$A = 8$

3) Node choose a secret integer b = 15, then sends the value of B to Base station

$B = g^b \bmod p$

$B = 5^{15} \bmod 23$

$B = 30{,}517{,}578{,}125 \bmod 23$

$B = 19$

4) Base station computes the $s = B^a \bmod p$

$s = 19^6 \bmod 23$

$s = 47{,}045{,}881 \bmod 23$

$s = 2$

5) Node computes the $s = A^b \bmod p$

$s = 8^{15} \bmod 23$

$s = 35{,}184{,}372{,}088{,}832 \bmod 23$

$s = 2$

VII. RESULTS

WSN security is one of the major concerns because of the lack of regular changing topologies. One of the major task is to design a security effective protocol that will help to avoid the attacks and provide a secure communication between the nodes. In a group communication security issues become worst because there are number of senders and number of receivers. So I am going to propose a new system that will be more efficient against the Black and DDOS attacks and helps to detect and prevent the attacks.

The proposed work will also enhance the performance of the network. The simulation is performed in Matlab.

A. Throughput

The following graph shows the comparison between the old work and new work in form of throughput. The new work shows the enhancement in the network in form of throughput.

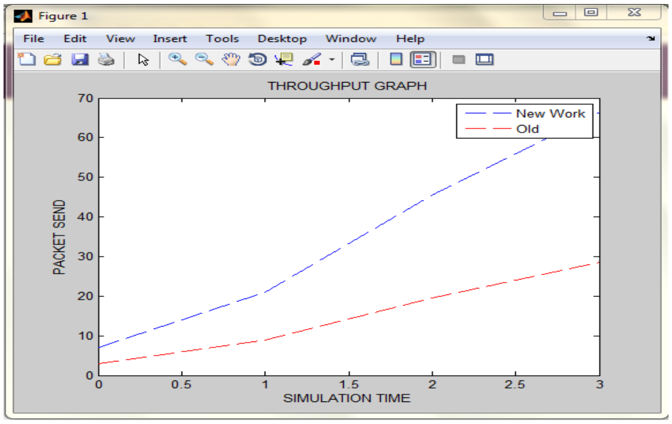


Figure 4: Throughput graph

B. Delay

The following graph shows the comparison between the old work and new work in form of delay. The new work shows the decrease in delay in the network.

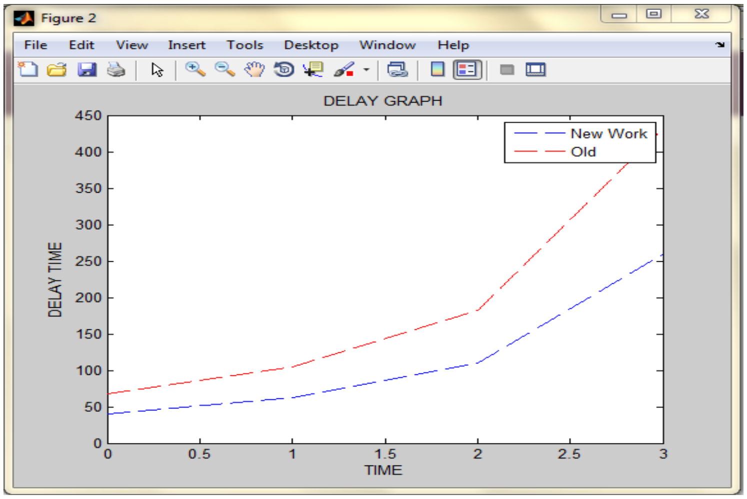


Figure 5: Delay graph

VIII. CONCLUSIONS

This proposed work is about the Wireless Sensor Network and security of it. The output of this work will be the detection and prevention of major attacks like Distributed Denial of Service, Black-Hole attack and Sybil attack. In this work we proposed a secure mechanism with based on some authentication steps related to Diffie-Hellman algorithm then mechanism will detecting and preventing Distributed denial of service, Black Hole, Sybil attacks using some network parameters mainly packet received, packet forwarded and battery power. Distributed Denial of Service attack forwarded large number of packets on the network and interrupt the legitimate nodes, whereas Black-Hole node dropped all the valuable packets and Sybil attack identity itself more than once at a time, So using this mechanism malicious node will detected and isolated or blocked for further communication on the network. A sensor network consisting from sensor node which deployed on the unreachable places. Every node made up with the sensing system, very less computational power and limited battery lifetime with many security problems. Sensor nodes sense the environment, process the data obtained by the node and forward this data to Base Station located some far from the sensor network through sink node. The study shows a secure mechanism which is based on some authentication steps related to Diffi-Hellman algorithm. Our mechanism is detecting and preventing Distributed denial of service, Black Hole, Sybil attacks and make wireless sensor network more reliable and secure for communication.

The future work of the study is to enhance the proposed technique to detect more such types of attacks like Gray hole attack and make wireless sensor network for secure for communication. The further implementation will include more WSN nodes and prevent the above discuss attacks.

REFERENCES

[1] Ahamed, SS Riaz. "The role of zigbee technology in future data communication system." Journal of theoretical and applied information technology, 2009: 129-135.

[2] Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. "Wireless sensor networks: a survey." Computer networks 38, no. 4, 2002: 393-422.

[3] Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." Ad hoc networks 1, no. 2 , 2003: 293-315.

[4] Kaur, Parminder, and Ravikant Sahu. " TO ENHANCE THE LIFETIME OF WIRELESS SENSOR NETWORK USING A NOVEL APPROACH BASED ON NEURAL NETWORK." ijcsme.com, 2014.

[5] Li, Xu, Amiya Nayak, and Ivan Stojmenovic. "Sink mobility in wireless sensor networks." Wireless Sensor and Actuator Networks, 2010: 153.

[6] Pathania, Shruti, and Parminder Singh. "Energy Efficient Mechanism to Enhance the Life Time of Wireless Sensor Network." ijaret.org, n.d.

[7] Petac, Eugen, Abdel Rahman Alzoubaidi, and Petrut Duma. "Some experimental results about security solutions against DDoS attacks." In Signals, Circuits and Systems (ISSCS), 2013 International Symposium on, pp. 1-4. IEEE, 2013.

[8] Sharma, Priyanka, and M. K. Rai. "Review paper on Cluster Based Caching Technique for Wireless Sensor Networks with multi-sink." International Journal for Advance Research in Engineering and Technology 1, no. 2, 2013.

[9] Sohraby, Kazem, Daniel Minoli, and Taieb Znati. "Wireless sensor networks: technology, protocols, and applications. ." John Wiley & Sons, 2007.