Early Detection of DDoS Attack in WSN

Kanchan Kaushal
CTIEMT
Shahpur
Jalandhar, India

Varsha Sahni
CTIEMT
Shahpur
Jalandhar, India

ABSTRACT
Wireless Sensor Networks carry out has great significance in many applications, such as battlefields surveillance, patient health monitoring, traffic control, home automation, environmental observation and building intrusion surveillance. However, wireless technology also creates new threats. Since WSNs communicate by using radio frequencies therefore the risk of interference is more than with wired networks. If the message to be passed is not in an encrypted form, or is encrypted by using a weak algorithm, the attacker can read it, and it is the compromise to the confidentiality. In this paper we describe the security goals and DDoS attack in WSNs. Most of the schemes are available for the detection of DDoS attacks in WSNs. But these schemes prevent the attack after the attack has been completely launched which leads to data loss and consumes resources of sensor nodes which are very limited. In this paper a new scheme early detection of DDoS attack in WSN has been introduced for the detection of DDoS attack. It will detect the attack on early stages so that data loss can be prevented and more energy can be reserved after the prevention of attacks. Performance of this scheme has been seen on the basis of throughput, packet delivery ratio, no. of packets flooded and remaining energy of the network.

General Terms
Network security, Attacks on WSN, Security mechanisms.

Keywords
Network security, Attacks on WSN, Security mechanisms, prevention of attacks from security threats.

1. INTRODUCTION
Wireless sensor networking remains one of the most demanding and ascending research areas of our time. A Wireless Sensor Network (WSN) is a collection of autonomous nodes, which transmits data in wireless channel with small bandwidth consumption and frequency.

Sensor networks hold a very well-known place in the history of technology due to the reason that they gives low cost solutions to a variety of applications such as data collection, scientific examination, military applications and monitoring. Each node can find out their neighbor nodes in network and this provide help in routes formation in the collection. Due to some weaknesses like limited processing memory, capability and due to broadcast transmission medium Wireless Sensor Networks are mostly vulnerable to Denial of Service attacks. These types of attacks reduce the capability of WSN, so that they cannot work for a long period of time. It has often effects on consumption resources in the network and increases the energy consumption, delay, and reduces the throughput.

A Denial of Service (DoS) attack is a type of attack with the purpose that genuine users are unable of using a particular resource of network that could be a website or/and whole system. A Distributed Denial of Service (DDoS) attack is a synchronized attack which is done on the availability of services of some particular network with the help of compromised computing systems indirectly, so that tracking the DDoS control packets becomes more difficult [3]. Figure 1 shows DoS attack on wireless sensor networks.

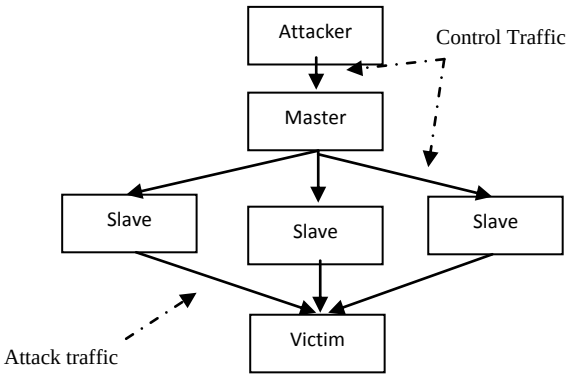

Fig 1: DoS Attack

The main aim of this paper is to protect the Wireless Sensor Network from flooding, a type of DoS attack. Flooding can exhaust all network resources such as bandwidth, energy and computing power etc. and design a new detection scheme named early detection of DoS attack using distributed technique. This scheme identifies the attacker on the basis of the number of transmissions corresponding to the number of neighbors of a node and these transmissions are compared with the threshold value computed and PDR of other nodes in the network.

The major contribution of this paper includes the introduction to wireless sensor network security and the flooding attack in section 2 and section 3 gives detailed information about related work that has been done in this field. Section 4 has explained the problem statement and criteria of attack detection is discussed in section 5. Section 6 has provided information about simulation environment and results and at last section 7 has mentioned the conclusion of paper.

2. SECURITY GOALS FOR WSN
As majority of sensor networks are deployed in hostile and dangerous environments with active intelligent opponent. Therefore security of Wireless sensor networks is a crucial issue. Primary goals of security of WSNs are; Confidentiality, Integration, Authentication and availability. There are some secondary goals of security such as Self-Organization, Data Freshness, Secure Localization and Time Synchronization.

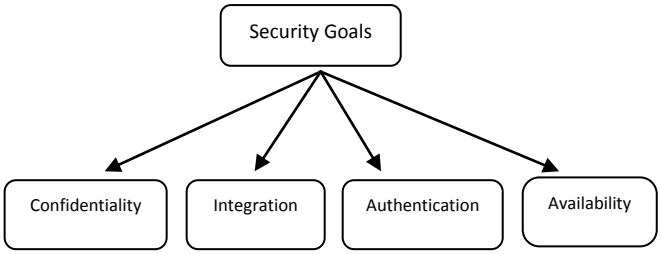

Fig 2: Security goals for WSN

2.1 Data Confidentiality

Many of the readings observed and produced by a sensor node can be distinguished as sensitive data, and hence, must get protection from eavesdropping by wretch sensors and intruders. A standard mechanism used for the protection of confidentiality of sensory data is to encrypt the message using cryptographic key. The resource constrained nature of sensor nodes makes it a difficult to create, store, and use the cryptographic keys of any kind, symmetric or asymmetric.

2.2 Data Authentication

The authentication of data transferred between the sensor nodes is mandatory to assure the protection against hoax messages that may be injected to the network by an adversarial node. Such type of attack might have catastrophic consequences considering the mission critical nature of sensor applications.

2.3 Data Integrity

Data integrity ensures that the received data is not modified or tampered with on its while transferring from sender to the receiver. For instance, in a bush are sensing network, an adversary may attempt to alter sensor readings to trigger an alarm which otherwise would have been initiated only for actual emergency scenarios. [3]

2.4 Data Availability

Sensor nodes placed in hostile environments to perform critical operations and they must be capable to outlast the expected battery lifetimes. Untimely exhaustion of the restricted battery lives of sensor nodes can have disastrous effects on operations of the whole network. Adversaries may try to introduce an attack against valuable resources in the sensor network to deplete their energy resources, and leads the network to be disabled from continuing to operate and perform its deputed functions involving to environment sensing and detection.

3. FLOODING ATTACK

Flooding attack is a type of Denial of service (DOS) attack and can deplete all the resources of the network such as bandwidth, energy and computing power etc so that network performance goes down and genuine user become unable to use network resources.

Flooding attack can be started by flooding the network with forged RREQ or data packets due to which network is completely jammed and the possibility of data broadcast of the authentic node is decreased.

3.1 RREQ flooding

In this type of flooding attack, the attacker broadcasts many RREQ packets to the node which can be survived or not in the network. To execute RREQ flooding the intruder increase the RREQ rate that destroys network's bandwidth and stop authentic users from using it.

3.2 Data flooding

In Data flooding data packets has been used to flood the network. In flooding attack, the attacker node first of all make a path to each nodes in the network and send the excessive amount of forged data packets and this forged data packet destroy the network's resources so that no one can use them and it will very hard to detect

4. RELATED WORK

[1] provides a scheme that check the profile of each node in network and only the attacker is one of the node that flooded the unnecessary packets in network then PPS has block the performance of attacker. The simulation results represent the same performance in case of normal routing and in case of PPS scheme; it means that the PPS scheme is effective and showing 0% infection in presence of attacker.

In [2]; two types of attacks on WSN that are jamming and flooding has been discussed and this paper provides an efficient technique for detection of flooding and jamming attacks. The method discussed in this paper provides improved performance over the existing methods.

Article [3] examines how attacks happen in WSNs and differentiate these attacks by conducting a survey. However, the main aim of this analysis is to examine how to prevent such attack in the WSNs by creating a sound understanding about various kinds of attacks in WSNs.

[4] has explored the WSN architecture according to the OSI model with some protocols in order to achieve good background on the wireless sensor networks and help readers to find a summary for ideas, protocols and problems towards an appropriate design model for WSNs.

[5] Gives idea that Denial of service (DoS) attacks can cause serious damage in resource constrained, wireless sensor networks (WSNs). This paper addresses an especially damaging form of DoS attack, called PDoS (Path-based Denial of Service). In a PDoS attack, an adversary overwhelms sensor nodes a long distance away by flooding a multihop end-to-end communication path with either replayed packets or injected spurious packets. This paper proposes a solution using one-way hash chains to protect end-to-end communications in WSNs against PDoS attacks. The proposed solution is lightweight, tolerates burst packet losses, and can easily be implemented in modern WSNs. The paper reports on performance measured from a prototype implementation.

In [6] Authors are conducting a review on DDoS attack to show its impact on networks and to present various defensive, detection and preventive measures adopted by researchers till now.

In [9], authors assess the security issues of wireless sensor networks with respect to medical applications and find out the possibility of a scenario when a distributed denial of service (DDoS) attack may be injected in the system using wormhole attack. They also propose schemes for detecting such attacks and also provide solution for its mitigation.

[10] Shows that the absence of central monitoring unit makes it vulnerable to several attacks. Denial of service attack (Dos) is an active internal attack which results in performance degradation of the wireless sensor network. This attack can be localized or distributed in nature based on intent of attack. In this paper, authors using modified variant of Ad-hoc On Demand Distance Vector (AODV) protocol to analyze the effect of Dos attack on system performance and later apply the prevention scheme to analyze the change in network performance.

[13] Traditional security schemes developed for sensor

networks are not suitable for cluster-based wireless sensor networks (WSNs) because of their susceptibility to Denial of Service (DoS) attacks. In this paper, authors provide a security scheme against DoS attacks (SSAD) in cluster-based WSNs. The scheme establishes trust management with energy character, which leads nodes to elect trusted cluster heads. Furthermore, a new type of vice cluster head node is proposed to detect betrayed cluster heads. Theoretical analyses and simulation results show that SSAD can prevent and detect malicious nodes with high probability of success.

5. METHODOLOGY

Sensor nodes monitor the environment and transmit the acquired data in a hop by hop manner to the destination node. The method will limit the number of transmissions of each node according to the number of their corresponding neighbors, so that no node can flood the data into the network. Step by step implementation of the proposed scheme has been given as following:

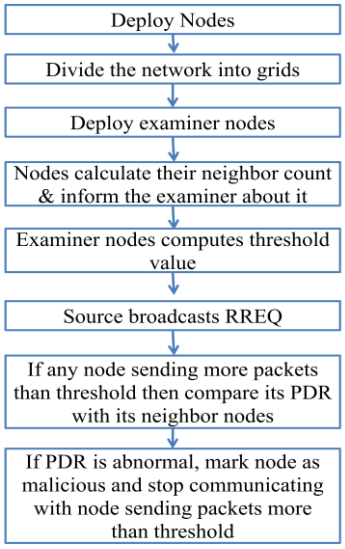

Fig 3: Steps for attack detection

Number of sensor nodes will be deployed in a specific area of region in a random topology. Then whole network will be divided into the grids. Each grid will have an examiner node. Each node will calculate its neighbor count and will inform to the examiner node, of their corresponding region, about it. Then examiner nodes will compute the threshold value of number of neighbors of each node. Source will broadcast the route request message to one of its neighbors. Examiner node will check if any node sending more packets than the threshold value then compares its Packet Delivery Ratio with its neighbor nodes. If any node flooding into the network, PDR of that particular node will be very high and If PDR is abnormal, examiner node will mark that node as malicious and the network will stop communicating with the node sending more packets than the threshold value. Repeat above three steps for every node in the network.

6. SIMULATION ENVIRONMENT AND RESULTS

The simulation is implemented In Network Simulator 2.31, a simulator for mobile ad hoc networks. The simulation parameters are provided in Table 1. We implement the random waypoint movement model for the simulation, in which a node starts at a random position, the simulation time is 30 seconds, and radio range is 250 meters. A packet size of 512 bytes and has cbr/udp type of traffic. Type of attack is DDoS attack and number of attacker will vary from 1 to 4.

Table 1. Simulation parameters for Case study

Examined Protocol	AODV
Number of nodes	56
Dimensions of simulated area	1000*1000
Simulation time (in seconds)	30
Radio range	250mtrs
Traffic type	Cbr/udp
Packet size (in bytes)	512
Types of attack	DDoS
DDoS attacker nodes	1,2,3,4

6.1 Performance Metrics

In our simulations we use several performance metrics to compare the proposed AODV protocol with the existing one. The following metrics were considered for the comparison were

6.1.1 Throughput: Number of packets sends in per unit of time. Throughput is measured in kbps.

6.1.2 Packet delivery fraction (PDF): The ratio between the numbers of packets sends by source nodes to the number of packets correctly received by the corresponding destination nodes.

6.1.3 Flood count: Flood count is number of packets flooded into the network by different number of attackers.

6.1.4 Remaining energy: Remaining energy is the energy remained in the network after the attack has been launched and prevented in the network.

6.2 Simulation results

In this section the analysis of simulation results are mentioned with different number of attackers. Table 1 shows the values of parameters Remaining Energy, packet delivery Ratio, Throughput and Flood count with respect to the different no of attackers.

Table 2. Parameters Vs No of attackers

	Remaining energy	PDR	Throughput	Flood count
1 Attacker	84.9701	0.560	63	1150
2 Attacker	84.85	0.555	65	1344
3 Attacker	84.7946	0.565	65	1538
4 Attacker	84.2156	0.5807	65	1926

6.2.1 Throughput Analysis: Number of packets sends in per unit of time. This graph represents throughput analysis in case when there is single attacker and then at two, three and four number of attackers. Throughput is measured in kbps.

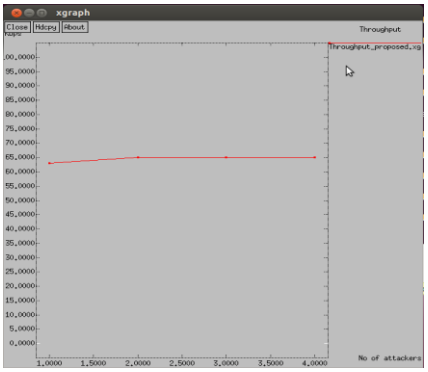

Fig 4: Throughput

6.2.2 Flood Count: Flood count is number of packets flooded into the network by different number of attackers. This graph shows the number of packets flooded by one attackers and then by two, three and four attackers.

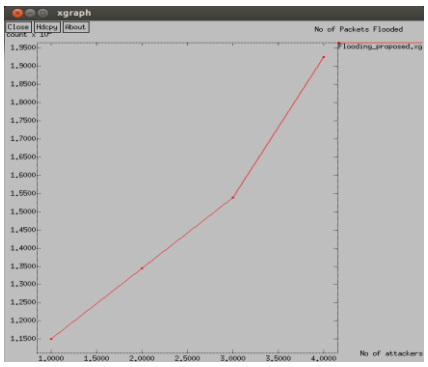

Fig 5: Flood count

6.2.3 Remaining Energy: Remaining energy is the energy remained in the network after the attack has been launched and prevented in the network. This graph shows the energy remained after the single attacker attacks to the network and then after two, three and four attackers respectively.

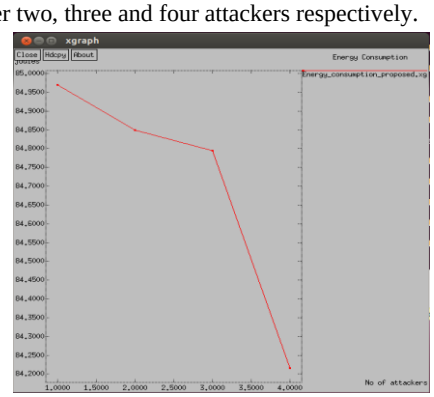

Fig 6: Remaining energy

6.2.4 Packet Delivery Ratio: The ratio between the numbers of packets sends by source nodes to the number of packets correctly received by the corresponding destination nodes. This graph represents PDR analysis in case when there is single attacker and then at two, three and four number of attackers.

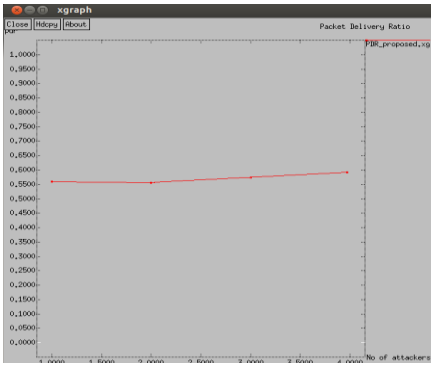

Fig 7: Packet delivery ratio

7. ACKNOWLEDGMENTS

The authors wish to thank the faculty from the computer science department at CTIEMT, Jalandhar for their continued support and feedback.

8. REFERENCES

[1] Varsha Nigam, Saurabh Jain and Dr. Kavita Burse, "Profile based Scheme against DDoS Attack in WSN", 2014 Fourth International Conference on Communication Systems and Network Technologies, IEEE, 2014.

[2] Shikha Jindal and Raman Maini "An Efficient Technique for Detection of Flooding and Jamming Attacks in Wireless Sensor Networks", International journal of computer applications, 0975-8887, Vol. 98, No. 10, 2014.

[3] Upavi .E.Vijay1, Nikhil Sameul2, "Study of Various Kinds of Attacks and Prevention Measures in WSN", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET),Vol. II, Special Issue X, March 2015.

[4] Ahmad Abed, Alhameed Alkhatib, and Gurvinder Singh Baicher "Wireless Sensor Network Architecture," International Conference on Computer Networks and Communication Systems, IPCSIT, vol. 35, 2012.

[5] Jing Deng, Richard Han, and Shivakant Mishra, "Defending against Path based DoS Attacks in Wireless Sensor Networks", *SASN'05,* 2005, Alexandria, Virginia, USA.

[6] Sonali Swetapadma Sahu et.a. "Distributed Denial of Service Attacks: A Review", I.J. Modern Education and Computer Science, 2014, 1, 65-71 Published Online January 2014 in MECS.

[7] Y.-C. Hu, A. Perrig, D.B. Johnson: Adriane: A Secure On-Demand Routing Protocol for Ad Hoc Networks, Annual ACM Int. Conference on Mobile Computing and Networking (MobiCom) 2002.

[8] K. Kifayat, M. Merabti, Q. Shi, D. Llewellyn-Jones: Group-based secure communication for large scale wireless sensor networks, J. Information Assurance Security. Vol 2, 139–147, 2007.

[9] Najma Farooq1, Irwa Zahoor2, Sandip Mandal3 and Taabish Gulzar4, "Systematic Analysis of DoS Attacks in Wireless Sensor Networks with Wormhole Injection", International Journal of Information and Computation Technology,Volume 4, Number 2 (2014), pp. 173-182.

[10] Ms. Shagun Chaudhary1, Mr. Prashant Thanvi2, "Performance Analysis of Modified AODV Protocol in Context of Denial of Service (Dos) Attack in Wireless Sensor Networks", International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015.

[11] Prajeet Sharma, Niresh Sharma, Rajdeep Singh, "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network", International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012.

[12] Saman Taghavi Zargar et.al. , "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, published online Feb. 2013.Guangjie Han, Wen Shen, Trung Q. Duong, Mohsen Guizani and Takahiro Hara , "A proposed security scheme against Denial of Service attacks in cluster-based wireless sensor networks", Security and Communication Networks,Published on 9 SEP 2011.