ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/91477, November 2016* ISSN (Online) : 0974-5645

Detection and Mitigation of Attacks in Cluster based Wireless Sensor Networks using Rule based IDS

J. Praveen* and V. Nithya

Department of Electronics and Communication Engineering, SRM University, Kattankulathur, Chennai - 603203, Tamil Nadu, India; praveenjay29@gmail.com, nithya.v@ktr.srmuniv.ac.in

Abstract

Objectives: Wireless Sensor Network (WSN) is made up of numerous small nodes; the node senses the happenings in its surroundings and reports the changes to a base station. Most of the sensor nodes are battery operated and their lifetime is less. **Methods/Statistical Analysis:** The WSN is operated in an open environment, it is prone to misuse. The misuse can either internal or external. External attackers can be prevented by using encryption techniques whereas the internal attackers being a compromised node in the network are hard to prevent. To avoid any further damage by the internal attackers an Intrusion Detection System (IDS) is developed. Rule based detection methodology is adapted to detect the misuse in the network. **Findings:** Using rule based detection methodology the following attacks such as black hole attack, selective forwarding attack, hello flood attack and replay attack are detected and mitigated. All the mentioned attacks occur in the network layer and its intention is to alter the data communication path. In a network of N nodes, M clusters are formed with each cluster having a cluster head. One node in each cluster has the IDS and monitors the cluster members before the communication starts. Once the attackers are detected within each cluster, the routing protocol is changed accordingly such that the affected cluster heads will not take part in the communication process. **Application/Improvements:** In existing IDS the attacks are only detected and by using some encryption they are prevented before an attack can happen. In this method the attacks are mitigated prior to the actual data transmission.

Keywords: Black Hole Attack, Clustered Wireless Sensor Networks, Hello Flood Attack, Intrusion Detection System, Rule based Detection, Selective Forwarding Attack

1. Introduction

In general, wireless sensor networks consist of abundant number of small-size, energy limited nodes stationed in a particular area, which is a self-organizing network formed by means of wireless communication[1]. Each sensor node in the network is responsible for aggregating the data from that particular area and transmitting the sensed data to the base station. With the fast growth in Information and Communication Technology (ICT), WSNs have been widely used[2]. The sensor network nodes are often stationed in forsaken and abandoned environment for a long time, which makes them prone to attack or invaded by an attacker, as a result, proposing a secured and simple intrusion detection system will be an essential and crucial step during the practical application of WSNs[3,4]. According to[5] types of intrusion in a network can be classified as masquerader, a person who is not allowed to access a network but tries to get access into the legitimate users account. Misfeasor, an authorized user who accesses the data which is not intended for them or the user who misuses his or her liberty. Clandestine user, a user who snatches supervisory control of the system and uses this control to dodge access controls. There are four main categories of intrusion detection techniques are available. They are rule based intrusion detection, Data mining and computational intelligence based intrusion detection, Game theoretical based intrusion detection, and Statistical based intrusion detection. In this paper, rule based detection methodology is used. In rule based IDS, the signatures of the previously known attacks are generated and are used as a reference

* *Author for correspondence*

to detect future attacks[6]. Few rules were defined in case of any deviation from the rule an attack in the network is detected. Rule based detection is suitable for WSN because they are easily put into practice and fit the demands of WSN resource curtailment. The various attacks that are detected in this paper are black hole attack, selective forwarding attack, hello flood attack and replay attack. These attacks occur in the network layer and they aim to affect the data transmission process. WSN have limited power resources so that having IDS in all nodes brings down the function period of the network. In order to deal with this, a clustered topology is used in this paper; in clustered topology, each cluster has a Cluster Head (CH) and Sensor Nodes (SN) as members. The cluster formation process finally leads to a two-level hierarchy where the CH nodes form the higher level and the cluster-member nodes form the lower level. The sensor nodes transmit their data to the corresponding CH nodes. The CH nodes aggregate the data and transmit them to the Base Station (BS) either directly or through the intermediate communication with other CH nodes. One node in each cluster has IDS, it monitors the other nodes in the cluster including the cluster head before communication starts and checks for any deviation in the rules, and in case of any deviation in the rules the node is marked as an intruder. Once all the intruders in the network are detected, the routing protocol is changed accordingly such that the affected node is in the path of data transmission. The paper is organized as follows, section 2 gives overview of the related works, and section 3 gives the description about the rules and attacks used in this paper. Section 4 gives the proposed work and the simulation results are discussed in section 5. Section 6 presents the conclusion.

2. Related Works

In the past few years many researchers have been working on intrusion detection system in wireless sensor networks.

In[7] the authors provide detailed information about IDS. A compendious survey of IDS for Mobile Ad-Hoc Networks (MANETs) is presented and applicability of those systems to WSNs is also discussed. Thirdly, IDSs proposed for WSNs are presented. The analysis and comparison of each scheme along with their advantages and disadvantages is also mentioned. A survey on various threats to WSN in different layers, the various advancements in securing a network and the challenges in implementing the advancements into the system are presented[8]. The attacks in the network layer are addressed in[8] are considered in our work.

In[9], a structural approach to the IDS is presented. It presents the essential features, advantages and disadvantages of each detection approach and the corresponding detection techniques. Withal, the authors also introduce the wireless intrusion protection systems. In[10], the authors have defined some rules for the detection of intrusion and these rules are used to identify any intrusion in the network. The authors also show that the attacks are detected accurately. The authors proposed IDS with intrusion prevention system.

The authors of[11] presents, a detection system for detecting black hole attacks using multiple base stations deployed in network by using mobile agents. Their proposed system is compared with the previous works. Probability of detection ratio of the black hole attacks is given graphically. In[12] the authors give the important limitations and damages of physical attacks at the network layer. The survey includes a comparison of various existing approaches for managing the security of WSNs on the network layer and their challenges for the implementation. Various approaches that are used for the detection of selective forwarding attacks in WSN are studied.

A mechanism in which sinkhole attack is detected using hop counting is proposed in[13]. The main advantage of this technique is that, a node can detect a destructive node only by associating with the neighboring nodes without requiring any connection with the base station. In[14] the authors proposed IDS based on node location verification algorithm for WSNs to detect the location of destructive nodes. In addition, the IDS detect hello flood attack and report the attack to the administrator. The result of this work is high detection ratio and low misdetection ratio.

Denial of service attacks such as flooding attack and gray hole attack are detected based on their energy consumption[15]. The authors used a light weight learning based energy prediction algorithm is used for the detection of flooding attack and gray hole attack in clustered WSN. In[16], the authors proposed a Multi Weight Based Clustering Algorithm (MWBCA) which is an extended

LEACH where cluster head is elected on weight given to each sensor node, then the collected data at cluster head is protected by using identity based Digital Signature. The authors showed that their work is more energy efficient when compared with LEACH. In[17], the authors used Network Intrusion Detection System (NIDS) along with signature based and anomaly based detection techniques. The monitoring is done at regular intervals, and by regular analysis, the attack is detected and the response is made once the attacker or intruder is detected.

The main contribution of our work is as follows. The internal attacks such as black hole attack, selective forwarding attack, hello flood attack and replay attack present in the network layer of a clustered WSN are detected using rule based detection technique. The detection of attacks is done before the data transmission takes place so that once the attacks in the network are detected; the affected nodes are excluded from the routing path.

3. Rules and Attacks

In this paper rule based IDS is used for the detection of attacks in the network layer. Because of the simplicity and efficiency in detecting the known attacks rule based IDS is used. From [10], the following rules are used to monitor the network for any intruders:

- Interval rule: Delay between the arrivals of two successive messages must be within definite limits.
- Retransmission rule: The transmitted messages should be redirected by the in between nodes.
- Integrity rule: The original message from the sender must not slew when it arrives at the receiver.
- Delay rule: The retransmission of a message must occur after a definite wait time.
- Radio transmission range: The messages should emerge from the neighboring nodes only.

In case of any violation from above rules, the activity can me marked as an unauthorized or intrusive and the node is marked as an intruder. The decision making can be done as combined or individually by the node or nodes. In combined decision making all the nodes take part in decision making whereas in an individual decision making only a single node's decision is considered as final. In this paper, we are using individual decision making. Based on the decision the node classifies the intruder as any one of the following four categories

- Affected node but not marked eccentric (false-negative): There is an intrusion in the system, but the IDS fail to detect it and decide the node as not eccentric one.
- Not an affected node but marked as eccentric (false-positive): There is no intrusion in the system, but the IDS mistakenly decide an unaffected node as an eccentric one.
- Not affected and not marked as eccentric (true-negative): There is no intrusion in the system, and the IDS conclude the node as non-eccentric one.
- Affected and marked as eccentric (true-positive): There is an intrusion in the system, and the IDS conclude the node as an eccentric one.

The various internal attacks[8] studied in this work are as follows,

- Black hole attack: The compromised nodes in the network occlude/drop the packets they receive instead of forwarding to them to the base station.
- Selective forwarding attack: The infected nodes try to stop the packets in network by repudiating to forward or simply dropping the messages passing through the node.
- Hello flood attack: The infected node broadcast the hello message to the whole network and attracts other nodes to choose this route for the data transmission.
- Replay attack: A valid data transmission is repeated or delayed by a node. An attacker copies the packets and forwards it later and continuously to the victim in order to exhaust the nodes energy.

4. Proposed Rule based Detection and Mitigation of Internal Attacks in WSN

4.1 Network Model

In this work, a WSN with 50 nodes consisting of 10 clusters, each cluster with 5 nodes is taken. One node is elected as cluster head and one node is the base station. All the data amassed by the cluster members are transmitted to base station via cluster head. If the base station is far away from the cluster head, the cluster head chooses a nearest cluster head and transmits the data to the base station through multi hop transmission.

4.2 Detection Technique

In the proposed detection method, a node in the cluster other than cluster head is selected as IDS randomly and before the data transmission starts, the IDS send few hello packets to the cluster member nodes and wait for certain time, based on the number of acknowledgements received, the type of the attack can be determined. The nature of the attacks and rules used to detect the attacks are detailed below.

4.2.1 Black Hole Attack

The affected node simply drops or blocks the packets they receive instead of forwarding them during black hole attack. The IDS sends 5 hello packets to each cluster member, if a node did not send any acknowledgement then the IDS detect it as black hole attack. The black hole attack can be detected using interval rule; delay between the arrivals of two successive messages must be within certain limits. The IDS wait for some after sending each hello packet and for receiving the acknowledgement.

4.2.2 Selective Forwarding Attack

The affected node simply drops or selectively forwards the packets they receive during selective forwarding attack. For the 5 hello packets sent, if the node send acknowledgements for 2nd and 3rd packet and doesn't send acknowledgements for the remaining packets, then the IDS detects the attack as a selective forwarding attack. The selective forwarding attack can be detected using interval rule; delay between the arrivals of two successive messages must be within certain limits.

4.2.3 Hello Flood Attack

The affected node sends many hello packets to the nodes in the network to attract the other nodes to send packets through them. For the 5 hello packets, if the node sends more than 5 acknowledgements then the IDS detects it as a hello flood attack. The hello flood attack can be detected using delay rule, the retransmission of a message must occur within a certain wait time.

4.2.4 Replay Attack

The packet transmitted is repeated or delayed by the infected node, the attacker copies a packet and forwards it later and continuously to a node to exhaust the nodes energy. For the 5 hello packets, if the node sends the same acknowledgement many times or the acknowledgement is delayed then the IDS detect it as a replay attack. The replay attack can be detected using integrity rule, delay between the arrivals of two successive messages must be within definite limits and delay rule, the retransmission of a message must occur within a definite wait time.

The various attacks and the rules used for detecting them are summarized in Table 1.

5. Simulation Results

5.1 Simulation Parameters

The scenario is implemented in network simulator 2; the following table shows the parameters used for the simulation.

Table 1. Attacks and the rules for detecting intrusion

Attack name	Description	Rule violation
Black hole attack	The compromised nodes in the network block/drop the packets they receive instead of forwarding to them to the base station.	Interval rule: delay between the arrivals of two consecutive messages must be within certain limits.
Selective forwarding attack	The infected nodes try to stop the packets in network by refusing to forward or simply dropping the messages passing through the node.	Interval rule: delay between the arrivals of two consecutive messages must be within certain limits.
Hello flood attack	The infected node broadcast the hello message to the whole network and attracts other nodes to choose this route for the data transmission.	Delay rule: the retransmission of a message must occur within a certain wait time.
Replay attack	A valid data transmission is repeated or delayed by a node. An attacker copies the packets and forwards it later and continuously to the victim in order to exhaust the nodes energy.	Delay rule: the retransmission of a message must occur within a certain wait time. Integrity rule: the original message from the sender must not deviate when it arrives at receiver.

Table 2. Simulation parameters

Parameters	Values
No. of nodes	50
No. of sink	1
No. of cluster heads	10
Routing protocol	AODV
Initial energy	10 J
Simulation time	100seconds
Delay rule waiting time	1 second
Interval rule waiting time	1 second

The above Figure shows the detection of black hole attack in the network, in the above Figure node 26 is the infected node, the routing protocol is changed such that the affected node doesn't involve in data communication process.

5.2 Simulation Results

Packet Delivery Ratio (PDR) is the ratio between the numbers of packets obtained at the receiver to the number of packets dispatched. The ideal PDR should be 100%. The following graph shows the PDR of various attacks with and without IDS in the network. The PDR of black hole attack is less because most of the packets are dropped by the infected node. In selective forwarding attack some packets are dropped and some are delivered. Hello flood attack and replay attack have similar PDR characteristics because the target of these attacks is to increase the delay of the transmission.

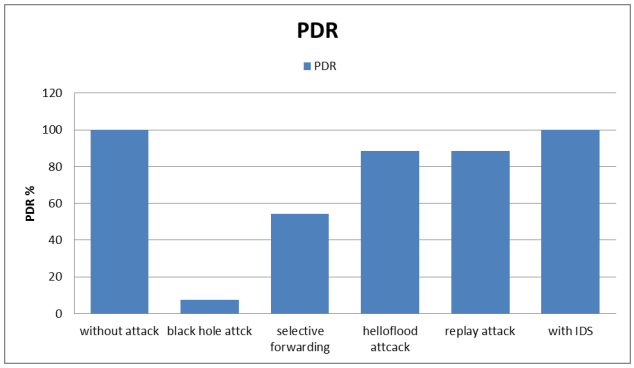

Figure 2. Comparison of PDR for various attacks in the WSN.

Residual energy is the energy that is left in the network after the process ends. The initial energy of the network is considered to be 10J; the energy left in the network after

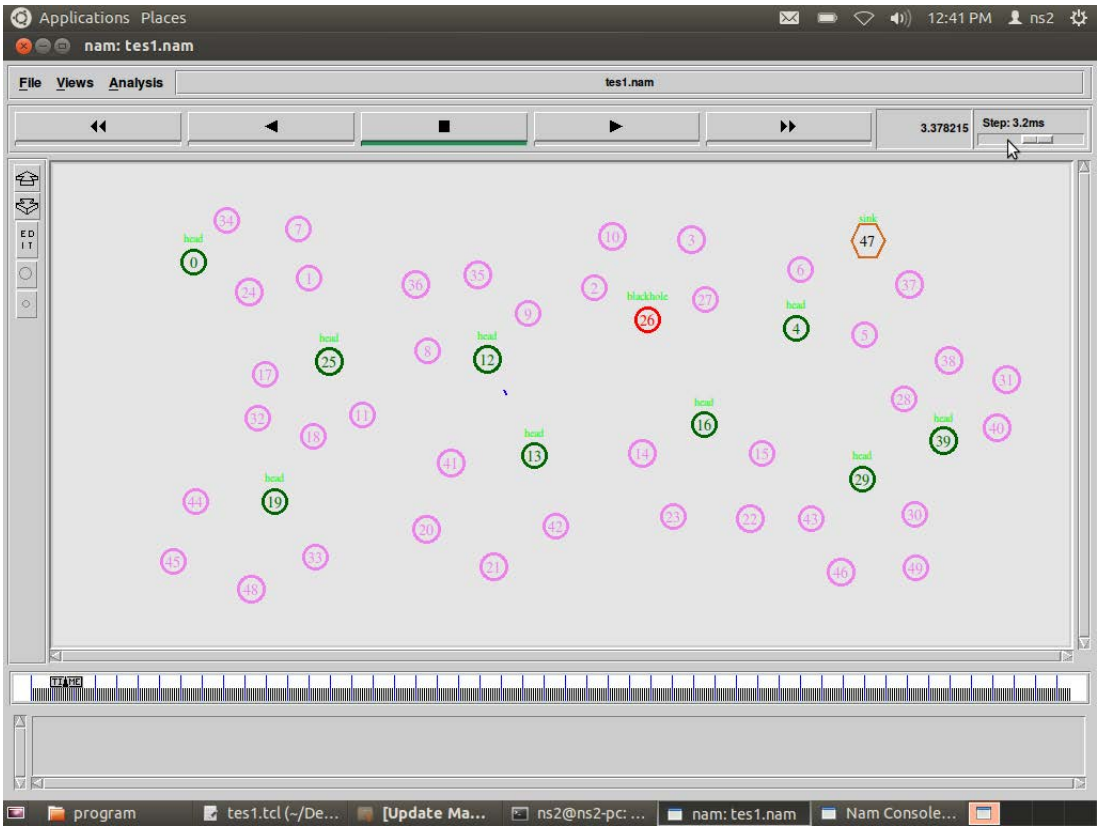

Figure 1. Detection of black hole attack in NAM file.

transmitting 12 packets is given in the graph shown below. For various attacks the residual energy is shown. Few joules of energy are spent in transmission of data, when the network is free of attacks the data packets reach the destination quickly. In black hole attack more energy is drained because most of the packets were dropped during this attack. During replay attack and hello flood attack the residual energy remains the same because they have similar characteristics in terms of action .When using IDS in the network the energy is reduced because the routing path is changed.

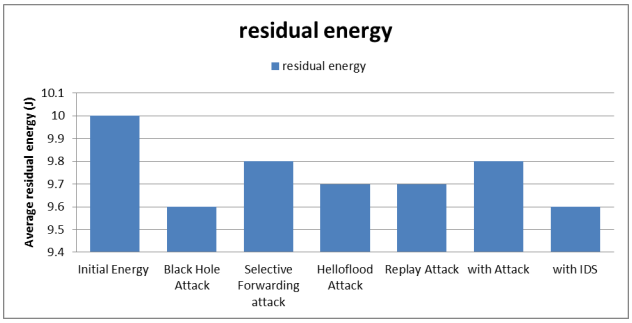

Figure 3. Comparison of residual energy for various attacks in the WSN.

Throughput is the rate of successful data that has been transferred to a destination or base station. The following graph shows the throughput of various attacks with and without IDS. Out of the 18000 bytes sent, in a network without any attacks all the bytes will reach the destination without any loss, when the network is affected by black hole attacks the throughput is decreased drastically. When the network is affected by selective forwarding the throughput is reduced by half. When the network is affected by hello flood attack or replay attack, the throughput is similar because the main target of this attack is to increase the delay of the data transmission.

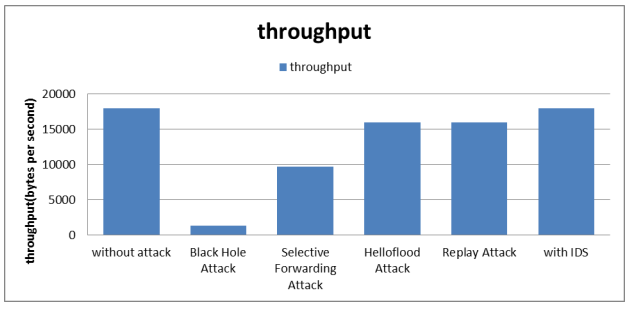

Figure 4. Comparison of throughput for various attacks in the WSN.

Delay is the time taken by the data packets from source to reach the destination. The delay for transmitting the packets in a network without any attack is less because the AODV routing protocol selects the shortest path to the destination from the source. In case of hello flood attack and replay attack the delay is increased because the infected node will be away from the routing path and it tries to attract the traffic to pass through them so the delay is high during these attacks. The delay is more when using IDS also because the routing protocol is changed accordingly such that the affected nodes doesn't involve in the communication process.

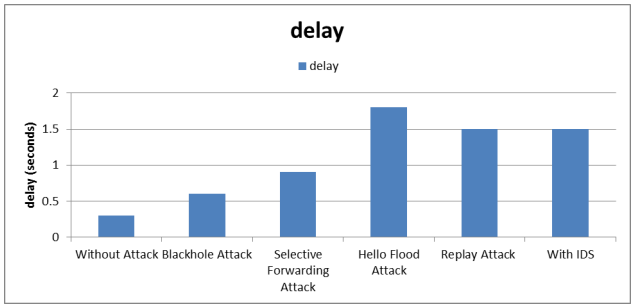

Figure 5. Comparison of delay for various attacks in the WSN.

6. Conclusion

In this paper, for a cluster based WSN we proposed a new acknowledgement based IDS using rule based detection technique for attacks like black hole attack, selective forwarding attack, hello flood attack and replay attack. The IDS detects the attacks before the data transmission takes place, once the attacks are detected the routing protocol is changed in such a way that the affected nodes will not receive any data. Only the unaffected nodes will participate in communication process. Therefore our proposed work not only detects the intrusion but also mitigates it before the actual data transmission. The performance of the IDS is studied using parameters such as throughput, packet delivery ratio, residual energy and delay.

7. References

1. Akyildiz F, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: A survey. Elsevier Science Computer Networks SA. 2002; 38:393-422.

2. Lu G, Xue W. Adaptive weighted fusion algorithm for monitoring system of forest fire based on wireless sensor networks. Conference on Computer Modeling and Simulation; Hainan. 2010. p. 414-7.
3. Alemdar A, Ibnkahla M. Wireless sensor networks: Applications and challenges. IEEE Signal Processing and its Applications. 2007:1-6.
4. Zhou Y, Fang Y. Security wireless sensor networks: A survey. IEEE Communications Survey and Tutorials. 2008:6-28.
5. Stallings W. Cryptography and network security, principles and practice. 5th ed. 2013.
6. Butun I, Morgera SD, Sankar R. A survey of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys and Tutorials; 2014; 16(1):266-82.
7. Venkatraman K, Daniel JV, Murugaboopathi G. Various attacks in wireless sensor network: Survey. IJSCE. 2013 Mar; 3(1):1-4.
8. Sobh TS. Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. Elsevier J Computer Standards and Interfaces. 2006 Mar; 28(6):670-94.
9. Deshmukh R, Deshmukh R, Sharma M. Rule-based and cluster-based intrusion detection technique for Wireless Sensor Network. International Journal of Computer Science and Mobile Computing. 2013 Jun; 2(6):1-9.
10. Sheela D, Srividhya VR, Begam A, Anjali, Chidanand GM. Detecting black hole attacks in Wireless Sensor Networks using mobile agent. International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012); Singapore. 2012 Jul 15-16. p. 1-4.
11. Alajmi NM, Elleithy KM. Comparative analysis of selective forwarding attacks over Wireless Sensor Networks. International Journal of Computer Applications. 2015 Feb; 111(14):1-12.
12. Md. Abdullah I, Rahman MM, Roy MC. Detecting sinkhole attacks in Wireless Sensor Network using hop count. I J Computer Network and Information Security. 2015; 3:50-6.
13. Hassoubah RS, Solaiman SM, Abdullah MA. Intrusion detection of hello flood attack in wsns using location verification scheme. International Journal of Computer and Communication Engineering. 2015 Feb 12; p. 1-10.
14. Dharini N, Balakrishnan R, Renold AP. Distributed detection of flooding and gray hole attacks in Wireless Sensor Network. International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM); Chennai, T.N., India; 2015 May 6-8. p. 178-84.
15. Palte RR, Satao R. Aggregated identity-based signature to transmit data securely and efficiently in clustered WSN. International Conference on Computing Communication Control and Automation; Pune, India. 2015 Feb 26-27. P. 138-42.
16. da Silva AP, Martins M, Rocha B, Loureiro A, Ruiz L, Wong HC. Decentralized intrusion detection in Wireless Sensor Networks. Proceedings of 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05); 2005 Oct.
17. Amudhavel J, Brindha V, Anantharaj B, Karthikeyan P, Bhuvaneswari B, Vasanthi M, Nivetha D, Vinodha D. A survey on intrusion detection system: State of the art review. Indian Journal of Science and Technology. 2016 Mar; 9(11):1-9.