ENHANCED GREEN FIREWALL FOR EFFICIENT DETECTION AND PREVENTION OF MOBILE INTRUDER USING GREYLISTING METHOD

G.Pradeep Kumar [1], R.Chakkaravarthy[2,]S.Arun kishorre[3], L.S.Sathiyamurthy[4]

1- Assistant Professor, ECE dept., Velammal College of Engineering & Technology, Madurai.
2 Final year students, ECE dept., Velammal College of Engineering & Technology, Madurai.

ABSTRACT:

Wireless sensor networks are nowadays widely popular and has become an integral part in the military applications for human monitoring, thermal detection etc. Security of Wireless sensor network (WSN) becomes a very important issue with the rapid development of WSN that is vulnerable to a wide range of attacks such as sinkhole attacks due to deployment in the hostile environment and having limited resources. Intrusion detection system is one of the major and efficient defensive methods against attacks in WSN. One such detection technique is black listing technology. But using only Black listing technology is not suitable for a mobile intruder since it was designed considering only a static intruding node in a WSN. So it is necessary to build an energy efficient Intrusion detection system for sinkhole attack by a mobile intruder in WSN. We are intended to design an energy efficient system for detection of sinkhole and elimination of a mobile intruder from WSN nodes using a technology called greylisting. This technology uses pre alarm packets to warn the neighboring nodes about the intruder and the energy consumed by the pre alarm packets for making an alarm is much lesser than that of the packets used in black listing technology. Thus this method will serve as the solution for the dilemma in providing the security for WSN in sinkhole attack.

1. INTRODUCTION:

Wireless Sensor Networks are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers, monitors the environment or system by measuring physical parameters such as temperature, pressure, humidity. Any disturbance caused by a node that is non-member to a particular cluster of nodes is said to be an intrusion.An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the cluster head about the intruder. There are many intrusion detection systems at present appealing 100% efficiency but the hard truth is that none of them could reach it. One of those steps towards a secure WSN is blacklisting technology. Blacklisting is the technology of maintaining a list of unauthorised nodes by the existing nodes in order to stop communication with those nodes. A node refers the blacklist when there is a need to communicate with a node or when there is a data transfer between those nodes. Though blacklisting is an efficient way of prevention of mobile intruder for maintaining the blacklist a lot of energy is consumed. This became a major drawback in the blacklisting technology.

DOI : 10.5121/ijist.2014.4313

In this paper we propose an enhanced green firewall using the greylisting technology for the energy efficient prevention of an intrusion by the mobile intruder.

- Green firewall uses greylisting technology which has less energy consumption compared to blacklisting.
- Enhanced green firewall checks and identifies the sinkhole attack and then blocks it using greylisting technology in an energy efficient manner.
- Pre-alarm packets are used instead of alarm packets to intimate the nodes in a cluster about the intruder in the network

2. RELATED WORK

2.1 sinkhole attack definition and detection

From the survey of Security Attacks in Wireless Sensor Networks done by Mr.ManishMPatel and Dr.AkshaiAggarwal Research Scholars in Gujarat Technological University, Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify.

As an example, a laptop-class adversary has a strong power radio transmitter that allows it to provide a high-quality route by transmitting with enough power to reach a wide area of the network. An approach to detect sinkhole attack using data consistency and network flow information is proposed in. It finds a list of suspected nodes and estimating the attacked area. Then using network flow graph, it effectively identifies the intruder in the list. Hop-count monitoring mechanism for detecting sinkhole attack is discussed in. Author has proposed Anomaly Detection System (ADS), which analyses the magnitude of hop- counts stored in a node’s routing table. Whenever any sensor node sends its message, all of four EM (Extra Monitor) nodes with high gain antenna will receive the message and RSSI value. If the destination of receive message is BS, then all of EM nodes will send RSSI value to the RSSI Based Sinkhole Detector to localize the position of the sender node.

After that the visual geographic map will be updated. If the flow of receive message does not correspond with normal flow of visual geographic map, then sinkhole attack will be detected. By monitoring the CPU usage of each node in fixed time interval, the base station calculates the difference of CPU usage of each node. After comparing the difference with a threshold, the base station would identify whether a node is malicious or not. Proposed routing algorithm uses mobile agents to collect information of all mobile sensor nodes to make every node aware of the entire network so that a valid node will not listen the cheating information from malicious or compromised node. It does not need any encryption or decryption mechanism to detect the sinkhole attack. Whenever a node advertises, it finds the digest of the message using the MD5/SHA1 algorithm, and sends it along the original path [30]. At the same time, send the message to the advertising node, which will either keep the message as it is if it is a trustable node, or alter the message if it is a sinkhole. This advertising node should then generate the digest for the message it is going to transmit and send it forward. The destination detects the attack only when the digest obtained from both the paths are different.

2.2 Blacklisting

From the paper Spectrum-Aware Wireless Sensor Networks done by Mr.Peng Du and Prof.George Roussos Dept. of Computer Science and Information Systems Birkbeck, University of London a blacklist consists of 16 bits that represent individual frequencies and channels are blacklisted by setting corresponding bits to 1. The sizing of blacklist controls the maximum number of channels allowed to exclude. This parameter can be either static or, alternatively, dynamic to cover any channel falling short of certain threshold, provided that at least one channel remains usable. The communication goes ahead if the prospective channel is not blacklisted; otherwise an alternative must be generated with Equation and checked again. This iterative process terminates when an admissible channel is found. Blacklists are periodically updated at intervals of Tu to reflect latest spectral condition. The synchronization of blacklists is crucial to maintaining communication between peers. In ADV slots, nodes insert their local blacklists to ADV payload and propagation is achieved simultaneously with standard TSCH timing synchronization. An important detail is that blacklisting is deactivated in ADV slots so that common hopping sequence can be easily recovered in case of desynchronized blacklists since ADV packets are always exchanged using default hopping sequence.

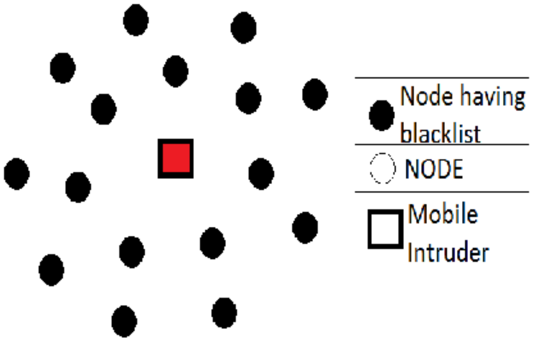


Figure 1: Blacklisting the entire region

3. ENHANCED GREEN FIREWALL

Before getting into the concept of enhanced green firewall it is necessary to define the following terms which are necessary to explain about green firewall and the way to enhance it. The following terms are coined in terms of wireless sensor networks which may differ from the original meaning of the term.

3.1 Blacklist

Every node contains a blacklist, which come from decision node. After receiving the alarm packet from its decision node, the node transfers the node in the alarm packet into the blacklist if it already exists in the greylist or adds it into its blacklist. As a result, it is guaranteed that every node would be informed before the intruder moves to it. Every node would defend against the intruder before it begins to attack. To the nodes listed in the blacklist, every node should block and isolate the node in blacklist.

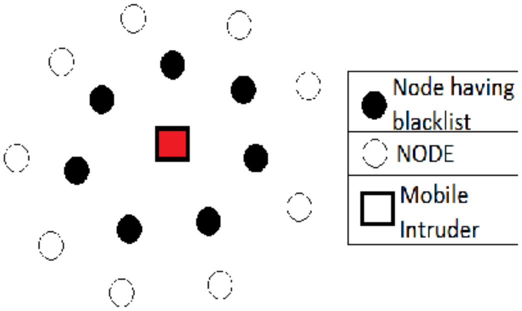


Figure2 : blacklisting the nearby nodes alone

3.3 Pre-alarm Packet

It includes node ID and is only broad- casted by normal node. The node broadcast a pre-alarm packet when it put one node into blacklist. A pre-alarm packet cannot be forwarded and it is not propagated for more than one hop. Neighbor nodes can receive the pre-alarm packet and put the intruder into greylist.

3.4 Alarm Packet

It include node ID and is only sent by decision node. Decision node regulates the pre-alarm list, which is used to count the pre-alarm packet from his cluster members. This list consists of two properties: node id and pre-alarm count. Once the decision node receives a pre-alarm packet from its cluster member, it adds the pre-alarm count of the corresponding node. When the pre-alarm count reaches the threshold, which is in proportion with the cluster size, it shows that an intruder has entered the cluster. The decision node conducts an alarm packet to its cluster members. Alarm packet is only sent by decision node and can not be forward by other node.

3.1 Greylist

Every node contains a greylist. Nodes in greylist come from pre-alarm packet broadcasted by other neighbors. A node put some node into its greylist when it receives node ID in pre-alarm packet from its neighbors. The node knows that the intruder in the greylist is close to itself, but the intruder may not enter its communication coverage. When the intruders enter its communication coverage, the node will transfer the intruder into blacklist and defence the intruder. In the meantime, the node broadcast pre-alarm packets include the intruder to its decision node and its neighbors.

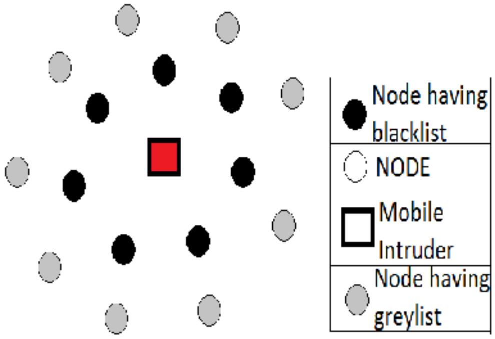


Figure 3 : Greylisting by sending pre alarm packets

3.5 Model of Green Firewall

When intrusion detection system finds an intruder in a WSN, it will inform every node in the WSN to isolate the intruder if the intruder is mobile. The method is to flood the alarm packet to all nodes in WSNs. It leads every node in the WSN to receive and forward the alarm packet, which consumes a lot of energy in network. Green firewall is used to protect WSNs against attacks in the networks with less energy consumption. The features of WSNs are multi-hop and wireless communication. A node receives and sends packets through its neighbor nodes. A node does not have connection with the other nodes in the network, if it's all neighbors cut off their links to it. The attacker has actually been isolated from the network even if it is still physically located in the network. The green firewall isolates the intruder by using the above principle. Green firewall need not broadcast the alarm packet to all nodes. Instead, it only broadcasts the alarm packet to the nodes which enclose the intruder. The method effectively reduces redundant alarm packets transmissions and meanwhile it decreases the energy consumption in WSNs

4. IMPLEMENTATION

We have implemented enhanced green firewall using JNS (Java Network Simulator). For a sample we have created 16 nodes and we have shown the sinkhole attack by a mobile intruder and the way it is detected and formation of a blacklist and also briefed about the formation of greylist and have compared the performance of greylist and blacklist.

4.1 Sinkhole detection

We use the concept of overhearing for sinkhole attack detection. Initially when a mobile intruder comes in as a sinkhole it transmits a packet to the nearby node in order to get the packets naming itself as one of the nodes in that cluster. In such cases the node will inform this to the cluster head, the cluster head in reply sends a "hello" packet to every node in that cluster. The original nodes of the cluster will reply for the message to the cluster head but the sinkhole will drop that packet which is its normal behaviour. Thus the cluster head comes to know that node is malicious and sends information about that node to all other nodes about the intruder in form of sinkhole.

4.2 Blacklisting and greylisting

After the detection of sinkhole the node is blacklisted only by the nearby nodes and greylisted by all the other nodes where there is a possibility of the intruder may move next. Thus continuous monitoring of all nodes is avoided and energy consumption is saved.

5. SIMULATION RESULTS

The major check here is the energy that is being used to implement green firewall and existing blacklisting technology. In order to check the energy being used in the blacklisting and green firewall we have to have some assumptions as follows.

Let us take the energy used for blacklisting as **Eb**

$E_b = E_i + \{\sum_i^n E_n\} + \{\sum_i^b E_b\} + E_m$The energy used for green firewall as **Eg**,
Where,
Ei- energy used for initial blacklisting
Ean- energy used by all nodes
Ebl- energy used after blacklisting
Em- energy used for maintaining and checking nodes with blacklist
Similarly we can calculate the energy used for Green firewall implementation,
Eg= Ei+Esn+Egl
Where,
Esn- energy used by specific nodes for monitoring
Egl- energy used for maintain the greylist
Thus from the above equations we can give dummy values and make an analysis by a chart between time and energy consumed as shown below.

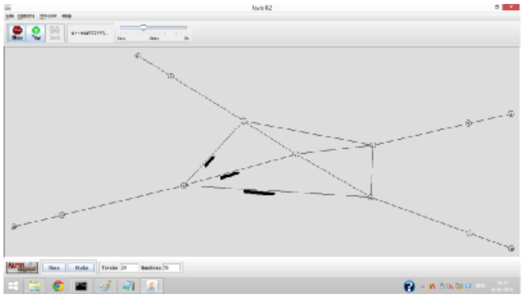


Figure4 :Step 1- sending hi packets to check for sinkhole detection

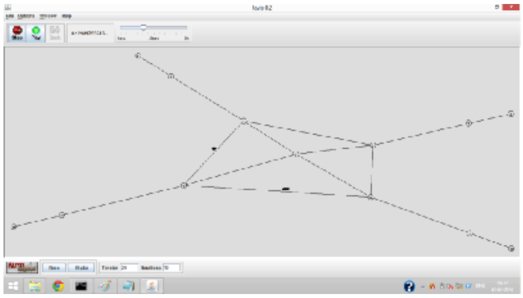
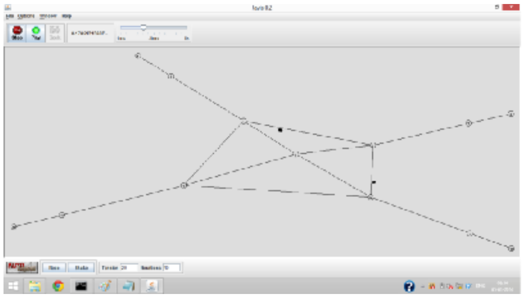


Figure 5 :Step 2- sinkhole



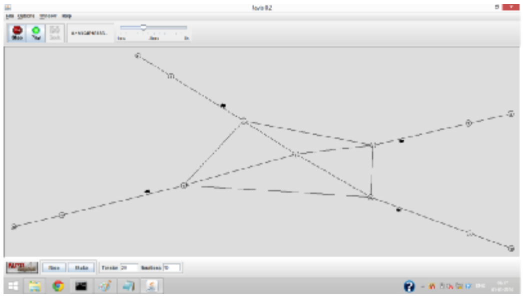
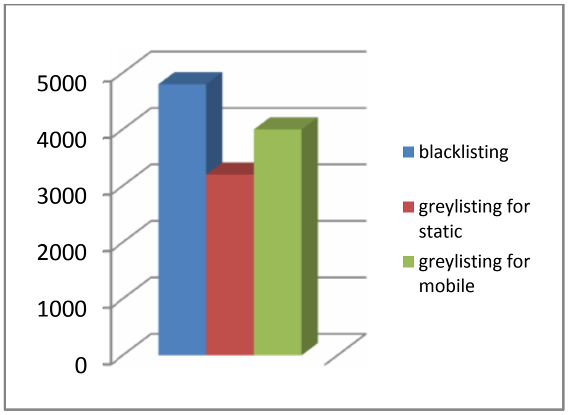


Figure 6: blacklisting by sending alarm packets Fig 7: greylisting by sending pre-
alarm packets

Energy comparison between enhanced green firewall and blacklisting



CONCLUSION

In this paper, we proposed an energy-efficient intrusion prevention mechanism in WSNs called green firewall to isolate the intruder. It includes two kinds of list: greylist and blacklist, and two kinds of packets: pre-alarm packet and alarm packet. We design their local propagating mechanism of these information to reduce energy consumption. We conducted theoretical analysis and compare it with the traditional flooding broadcast blacklist. To reveal the performance of green firewall, we also performed extensive simulation with five representative scenarios: static, crossing movement, short- distance movement, long-distance movement, and multipleintruders. The results show that the green firewall can provide low control overhead by reducing the number of alarm packet transmissions, green firewall can effectively reduce the energy consumption and make it an energy-efficient intrusion prevention mechanism in WSNs.

REFERENCES

[1] Detection of sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms, S.Sharmila and DrGUmamaheswari978-1-61284-764-1/11/$26.00 ©2011 IEEE

[2] A Sinkhole Attack Detection Scheme in Mintroute Wireless Sensor Networks, Murad A. Rassam, AnazidaZainal, Mohd. AizainiMaarof, and Mohammed Al-Shaboti, 2978-1-4673-4786-0/12/$31.00 ©2012 IEEE

[3] A Non cryptographic method of sink hole attack detection in wireless sensor networks, D.Sheela, Naveen kumar. C and Dr. G.Mahadevan, 978-1-4577-0590-8/11/$26.00 ©2011 IEEE

[4] Improved Two-factor User Authentication in Wireless Sensor Networks, BinodVaidya, DimitriosMakrakis, Hussein T. Mouftah, 978-1-4244-7742-5/10/$26.00 ©2010 IEEE

[5] Node Localization in WSN Based on Weighted Vectors Centroid Algorithm,Xiaoqin Su, Zhaoming Lei, 978-0-7695-4543-1/11 $25.00 © 2011 IEEE

[6] Security Attacks in Wireless Sensor Networks: A Survey, Mr. Manish M Patel , Dr.AkshaiAggarwal, 978-1-4799-0317-7/13/$31.00©2013 IEEE

[7] Spectrum-Aware Wireless Sensor Networks, Peng Du, prof.Georgebroussous, 978-1-4577-1348-4/13/$31.00 ©2013 IEEE

[8] AshfaqHussainFarooqi, FarrukhAslamKhan ,Jin Wang Sungyoung Lee (2012) A novel intrusion detection framework for wireless sensor networks, Pervasive Ubiquitous Computing DOI 10.1007/s00779- 012-0529-y, 2012.

[9] Y. Zhou, Y.G Fang, Y.C. Zhang, Securing Wireless Sensor Networks: a Survey, IEEE Communications Surveys & Tutorials, 2008, Vol.10, No.8, pp.6-28

[10] Jinsong Wu, Honggang Hu, Murat Uysal, High-Rate Distributed Space- Time-Frequency Coding for Wireless Cooperative Networks, IEEE Trans- actions on Wireless Communications, 2011, Vol.10, No.2, pp.614-625

[11] K.Ren, W.Lou, K.Zeng, P.J.Moran, On Broadcast Authentication in Wire- less Sensor Networks,IEEE Transactions on Wireless Communications, 2007, Vol.6, No.11, pp.4136-4144