DETECTION OF BLACKHOLE ATTACK IN IOT

Sweta Kale[1] Dr. Snehal Bhosale[2]
[1,2] RMD Sinhgad School of Engineering

Abstract

In near future, the number of IoT devices connected to internet will increase because of more applications arising in Internet of Things (IOT). Adding security in such devices is very challenging due to its resource constrained and nature of these devices with respect to battery and processing power. That is why he wormhole attack, sinkhole attack, hello flooding attack, Cybil and clone ID attack all such types of attacks take place in IoT. Black hole attack which is recently discovered can be launched against any protocol. Also its ability to be effective in case of encrypted traffic makes these attacks very severe and challenging.

Likewise Wormhole attack can cause failure of location dependent protocol, which may enter wrong route/topology information misleading the purpose of routing algorithm

A method to identify the black hole attack taking place at routing layer of IOT and Intrusion Detection system for it is proposed in this paper.

Introduction

1.1 Internet of Things

Due to advancement in computing and communication IoT is recognised as a trend for causing a global change. Due to user to machine interaction and machine to machine interaction has lead to transform IoT. Many IoT product including healthcare, energy, automotive and agriculture have already captured and made their place in the market.

Devices such as exercise fit bits, robots, and insulin pumps have become more connected to one another with IoT. A positive transformation is expected by IoT in the way how we live along with significant changes in industrial sectors. By incorporating IoT better standards of living can be aimed, by various value creations opportunities and improving the careers of many. A web of new smart paradigms like smart healthcare, smart agriculture and smart power is expected by adapting IoT. This may emerge into a new ecosystem of IoT which will be driven by self-aware automatic machine. The world is going to become a better place to live with more communication with everyone. In near future large number of devices will be connected to the internet due to increasing use of internet in day to day life and this will provide great facilities to the world. IoT is creating a new era of innovation that connects the digital and machine ecosystems and brings better speed and effectiveness to many sectors which are stated above. Due to this there will always be a risk to the Industrial Control Systems (ICSs) and to other connected online, due to communication of devices with one another. Addressing the challenges and ensuring security in IoT products and services must be a fundamental priority of end users. Poorly secured IoT devices and services can serve as potential entry points for cyber attack and expose user data to theft[1].

However with the sensitive information increasingly being made available online by more use of IoT devices may lead to several attacks and theft. This has leaded the research community to thing that security cannot be ignored. The packets that move across heterogeneous networks and are thus susceptible to various attacks common to both the digital and machine world[2]. At this stage the security challenges need to be addressed to achieve success with the use of various application of IoT. The objective of this research is to develop a lightweight trust-based Routing Protocol

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

for low power and Lossy networks (RPL) that will address one of the many attacks black hole attacks in IoT[2]. We have shown that our proposed system is secure from black hole attacks without imposing undue overheads on network traffic. We present our simulation results using the Matlab environment.

1.2 Security in IoT

Ever since the beginning of communication of two computers data protection has always been a great concern. Now a day's internet has been commercialized and due to this the security issues has been a major problem related with personal privacy financial transactions, and the threat of cyber theft. It has been estimated that there will be more than 41 billion connected IoT devices by 2025. The reliability and safety of IoT products depend on robust, end-to-end security approaches.

Security and safety are inseparable in IoT. Whether accidental or malicious, interference with the controls of a car or in nuclear reactor can be a threat to human life. As tremendous evolution in network is being taking place, security controls have also evolved right from the first packet-filtering firewalls in the late 1980s to more sophisticated protocol- and application-aware firewalls, intrusion detection and prevention systems (IDS/IPS), and security incident and event management (SIEM) solutions. If malicious activity tries to take control of the network, these systems try to detect them. Antivirus techniques based on signature matching and blacklisting may lead to identify and provide the solution to the problem caused if malware managed to break a firewall.

Later as the malware expanded and so as the techniques for avoiding detection advanced, white listing techniques started replacing blacklisting. Various access control systems were developed to authenticate the device and the user. IoT manufacturers are more eager to produce and deliver their devices as fast as they can, without giving security a priority concern. Various software verifications techniques was always a concern due to protection of intellectual property. 802 .11i (WPA2) or 802 .1AE (MAC sec), have developed to ensure the security of data in motion. All tough the confidentiality of data will always remain a primary concern to the manufacturer.

Security must be addressed throughout the device lifecycle, from the initial design to the operational environment. Below are the listed few aspects that need to be considered:

- Wireless mobile ad hoc networks strive for the security threat know as black hole attack.
- In black hole attack a malicious node uses its routing protocol in order to state that it has the shortest path to the destination. But eventually it drops the packet and does not fwd to the neighbouring node which leads to data loss.
- A malicious node replies with PREQ packet stating that it has the shortest path, from the source node to destination node.
- The mobile ad hoc networks are more vulnerable to single black hole attack.

Effects of attacks

- Traffic analysis for information leaking.
- Routing description.
- Drop data packets.
- Bypass and attracts large amount of network traffic.

Detection Schemes:

- Neighbourhood based and route recovery scheme
- Redundant route method and unique sequence scheme
- Time based threshold detection scheme
- Random two hop ACK
- Resource efficient accountability scheme
- Detection ,prevention and reactive scheme

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

- Next hop information scheme

Black hole Attack:

- In Black hole attack, a malicious node states to have a shortest route to the destination. But this node may drop all the packets that it receives for forwarding to its neighbour. When the black hole node is also a sinkhole it becomes more threat, as such an attack combination may stop all the data traffic around the black hole.
- During the BH attack, the node blocks / drops incoming data instead of sending towards the receiver [4]. Black hole is the malicious behaviour of a node claiming that it has the smallest path towards the destination. The purpose of a Black Hole attack is to drop the incoming data packets [5].

Literature Survey

Taylor Vincent F, Fokum Daniel T discussed IoT is autonomous self organizing, low power nodes which measures data in an environment and cooperate to route this data to its destination. On wireless sensor networks Black hole attacks are disturbing attacks.
It uses false route, it tries to attract network movement by stating that it has the shortest path and then it drops the packet, so the author has proposed a robust and flexible attack detection scheme. The scheme uses a watchdog mechanism and lightweight expert system on every node to detect anomalies in the behaviour of neighbouring nodes. By using this method great node will have the capacity to identify them based on their behaviour. Even though if there is a possibility of malicious node getting inserted into the network. By utilizing simulation the authors have examined the resource-preserving mechanisms. They have demonstrated that group of nodes are allowed for overall evaluation of network activity and identify attacks, by making use of limited hardware resources (handling, memory and capacity) that are typically accessible on wireless sensor network nodes [3]

Binod Kumar Mishra et.al presented that Wireless sensor is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner. They monitor and control over physical or environmental conditions, like pressure, sound and temperature. Applications for the development of security in wireless sensor networks were required to be developed. Today such networks are being utilized in many areas. When an intermediate node 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 black hole attack take place. Many techniques have been proposed for detection and prevention of black hole attack in sensor network [4]

Chun–Hsin Wang and Yang-Tang Li suggests, that many network security problems exist in MANET, as nodes in MANET are free to move randomly as the network topology changes frequently. The malicious node can drop, modify or even steal the data packets [5]. This happens when the malicious node states that it has a shortest path to reach to the destination. When the packet arrives to the malicious node it either drops the packet or does not forward to the neighbour node. This lead to data loss and unnecessary use of bandwidth. Many works on how to handle the malicious node problem has been proposed in this literature. Such type of work exits in Thakur et al., International Journal of International Journal of Advanced Research in Computer Science and Software Engineering 7(4), April-2017, pp. 393-397 © 2017, IJARCSSE.

Medadian Mehdi et.al describes [6] that MANET is a network in which nodes are

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

free to move and communicate with each other. The nodes need to cooperate with each other for proper network functionality. AODV (Ad hoc on demand Distance Vector) is a loop-free routing protocol for ad-hoc network. Ad hoc routing protocols are developed under the assumption that the collaborating nodes are friendly and cooperative. Due to this the networks are always vulnerable to different attacks which may lead to the data loss. Black Hole' attack is a threat to AODV. In Black hole attack, a malicious node states to have a shortest route to the destination. But this node may drop all the packets that it receives for forwarding to its neighbour. A solution to this is to wait and check replies from all the neighbouring nodes as this may lead to the authenticate route for delivery of packets. But the disadvantage is delay by using this process. A negotiation approach is proposed to overcome the Black hole attack. This protocol achieves better performance and better security.

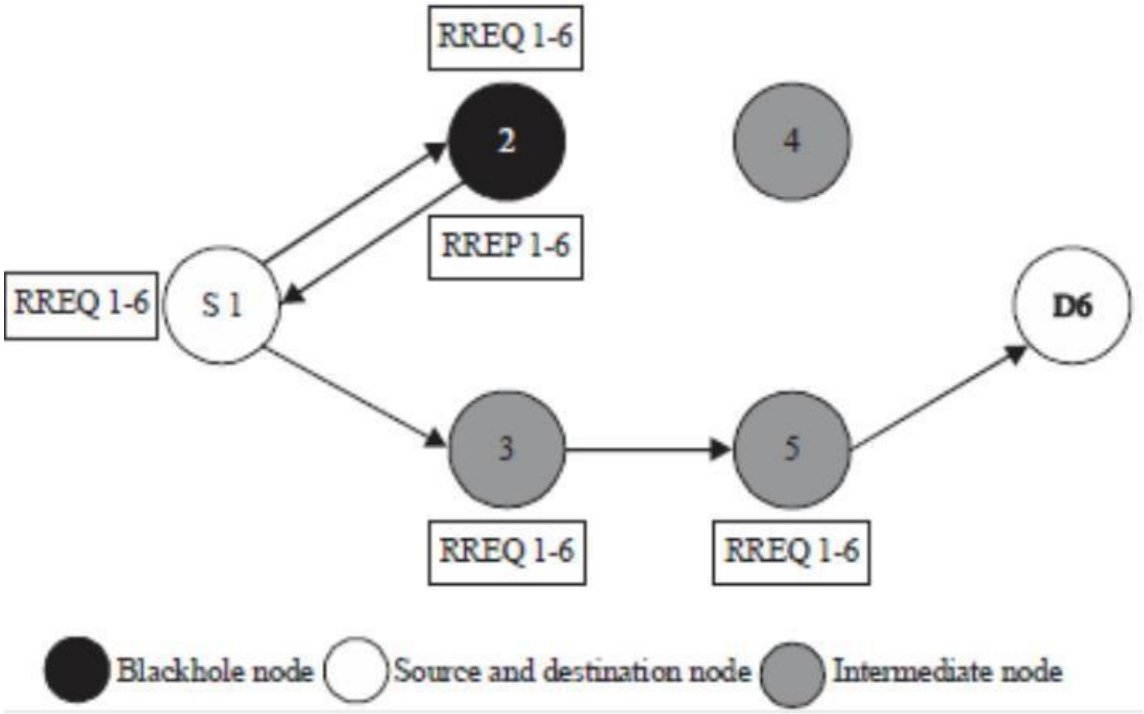


Figure 1: Black hole attack

Wireless mobile and ad hoc networks are more vulnerable to different attacks. Black hole attack is one of the well-known security threats[7]. In Black hole attack, a malicious node states to have a shortest route to the destination. But this node may drop all the packets that it receives for forwarding to its neighbour. A node who replies with RPEQ packet sent form source node, is a false response created by the malicious node. A single black hole attack can easily happen.[8]

DESCRIPTION

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

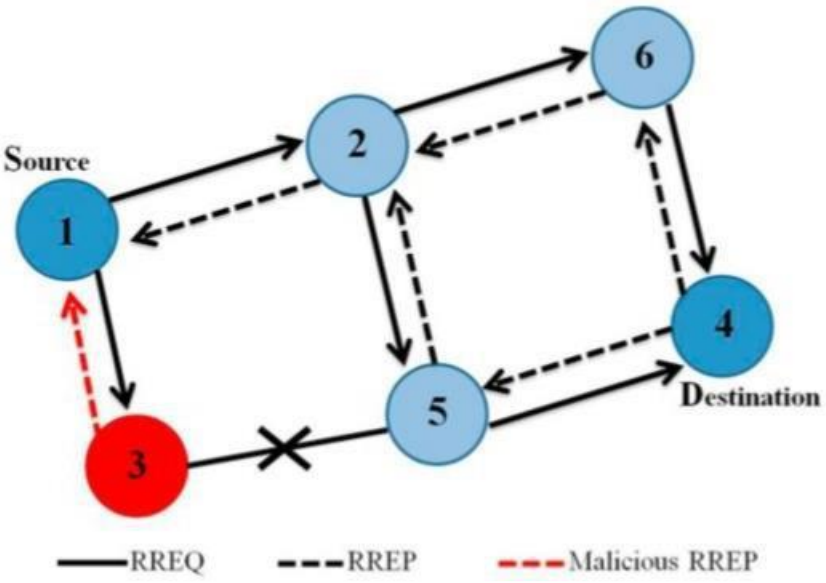


Figure 2: Description of Black hole attack

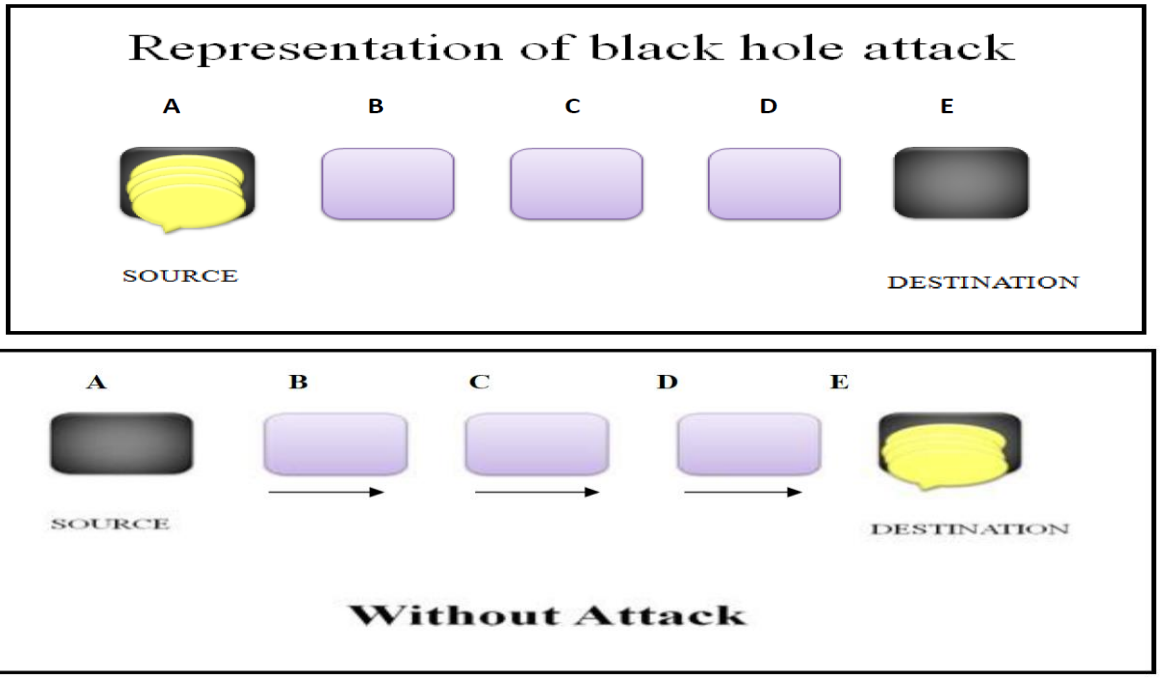
In the Figure 2, node 1 is the source node and node 4 is destination node. When the packets travel form source node to destination node during this the attack can take place.

A node can acts as a misbehaviour node and make a false response that it has a shortest path to destination. Here in the above figure node 3 is a misbehaviour node. Therefore node 1 gets a false completion route and starts to send packets to node 3.

The misbehaviour node starts to drop the packets and this is the black hole attack problem in MANET. So the node 3 misguides the delivery of packets in the networks. So the network can suffer the delay.

REPRESENTATION

:



ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

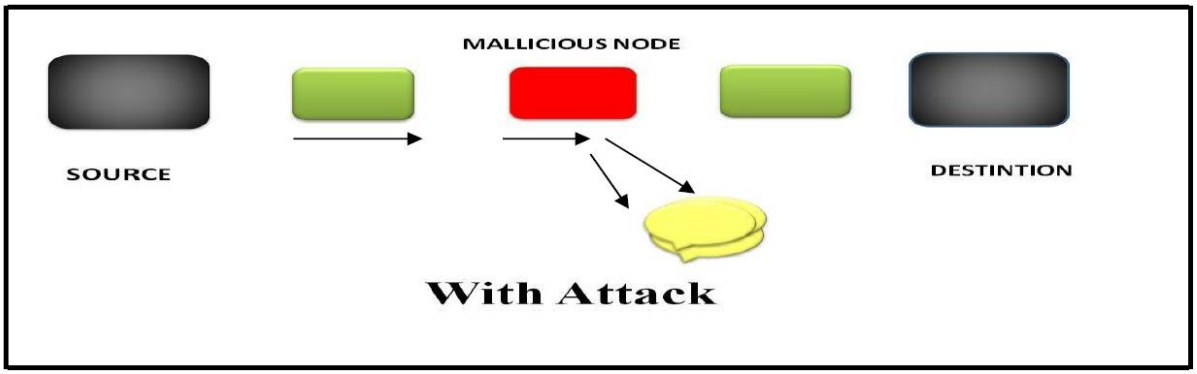


Figure 3: Representation of Black hole Attack

PROPOSED SOLUTION FOR BLACK HOLE

The mechanism used to defend the system against a black hole attack is discussed. In order to proceed further a necessary assumption is that the base station (BS) is trustworthy. This is a basic requirement to facilitate a decision whether a node is malicious or normal as it rules out BS involvement in the attack.

The method to determine if a node is malicious or not is divided into two phases

1. Pre-deployment phase

The access point is in range with its base station(BS). Due to this the distribution of unique random numbers from the BS to APs can be done easily. Contiki's pseudo-random number generator and a custom seed generator is used for generating numbers. In this it is assumed that no malicious node is active and the delivery of packet is in controlled manner. Figure 4 illustrates the initial phase of the system.

After the completion of this phase if there is a requirement for AP addition it can only be done for the APs that are not acting as source nodes (data senders). The mechanism necessary for re-authenticating the source APs is proposed for future work and is not covered in this paper.

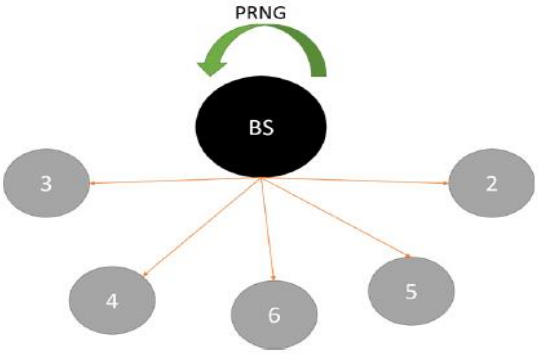


Figure 4. Pre-Deployment process: The access points receiving their respective unique random numbers from the BS.

2.Routing phase:

The routing protocol is modified to suit the needs of our medical WSN system. The first modification is the reversal of the senders of RREQ and RREP packets , i.e., the destination node (BS) sends RREQ packet and the source node (Ni) replies with a RREP packet, figure 5. shows the modification and has the following advantages:

1. Reduced network traffic compared to original AODV protocol because an

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

attacker cannot flood the network with bogus RREQ packets, thus reducing the chances of a DoS attack.
2. The network is controlled by the base station which is capable of setting the data intervals for the access points, thus an attacker is incapable of changing the data interval, thereby reducing further possibility of a DoS attack.

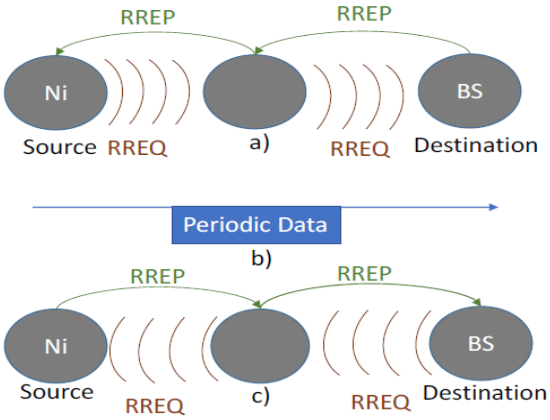


Figure 5. Routing Phase: (**a**) AODV protocol; (**b**) data direction; and (**c**) modification for our system.

The routing process starts when the BS requires data, this may be the case when an external request (by the staff) or an automatic periodic request (by the BS) is made. When the BS recognises that it needs patient data, it sends a request to the source node Ni using the RREQ packet.

destination	RREQ_ID	pad
interval		flag
$Q = H(r_i \| TS)$		

Figure 6. RREQ Packet.

In the above figure the RPEQ packet consist of a Q named field, where Q=H(ri || TS). Where H is SHA2 hash algorithm, ri is random number for the give node and TS is the time stamp. The modification made helps in source authentication. This in turns lead to attack prevention.
The former implication gives the assurance regarding the RREQ packet and the later implication states that an adversary cannot reply old message to facilitate penetrating the routing path.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

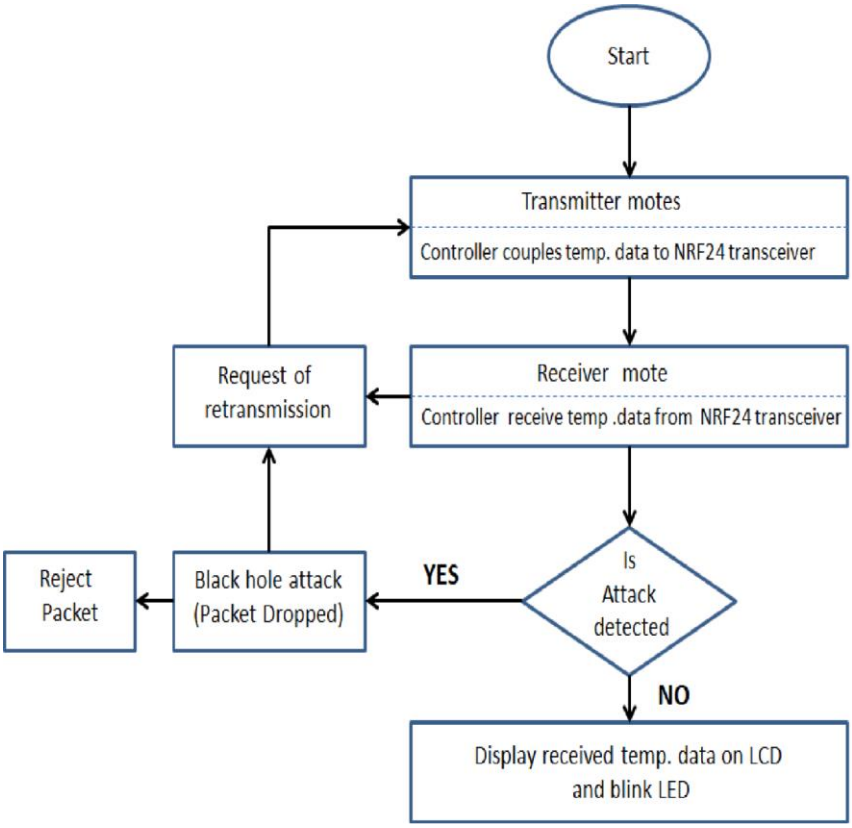


Figure 7: Flow chart for black hole attack detection

SOFTWARE REQUREMENTS:

MATLAB SIMULINK :-

Simulink is a MATLAB-based graphical programming environment for modeling, simulating and analyzing, model-based design environment for dynamic and embedded systems, model-based design environment for dynamic and embedded systems, integrated with MATLAB.

It is developed by Math works. It contains a customizable set of block libraries and contains a graphical block diagram tool. MATLAB algorithms can be used in this model and the results generated by simulation can be used by MATLAB for further analysis.

Simulink supports −

- system-level design
- simulation
- automatic code generation
- testing and verification of embedded systems

Simulink can use several other add-on products provided by Math Works.

Following is the list with the description given below–

 State flow: This allows us to develop state machine and flow chart.

 Simulink Coder: By using **t**his the generation of C source code for real-time implementation of systems can be done automatically.

 xPC Target together with **x86-based real-time systems:** With the help of this a environment is provided to simulate and test Simulink and State flow models in real-time on the physical system.

 Embedded Coder: When specific embedded targets are to be used this can be utilized.

 HDL Coder: By making use of this we can generate synthesizable VHDL and Verilog automatically.

 SimEvents : When modelling queuing systems is to be used this provides a library of graphical building blocks.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

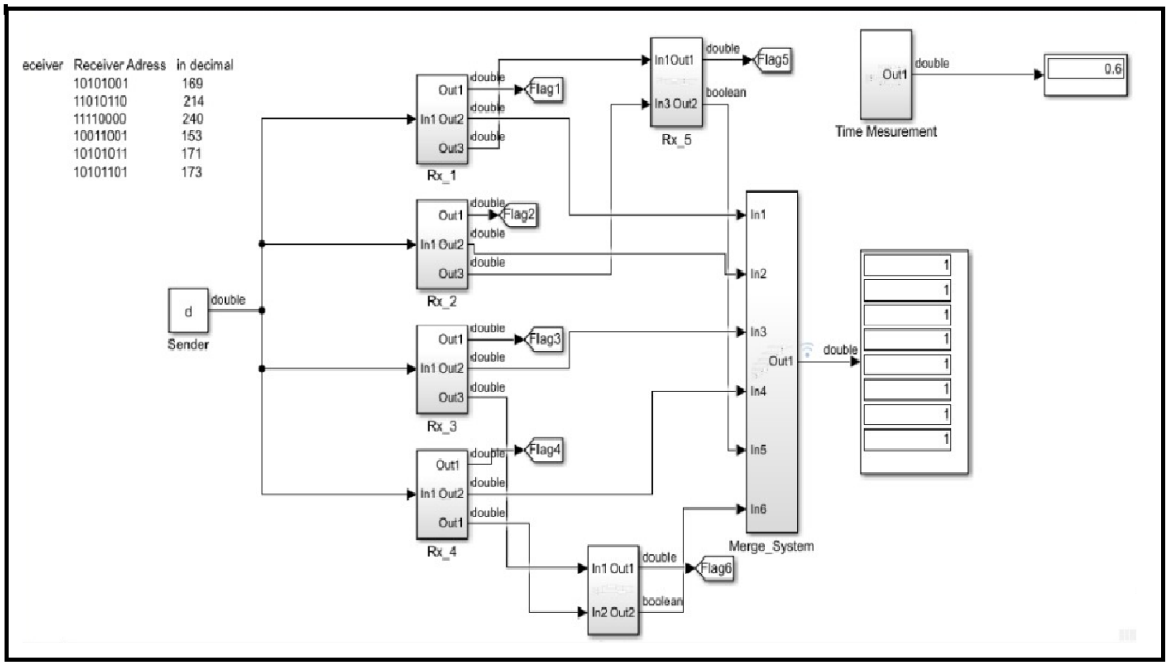


Figure 8: Simulink for Black hole attack

Conclusion

In Black hole attack, a malicious node states to have a shortest route to the destination. But this node may drop all the packets that it receives for forwarding to its neighbour. The networks suffer a huge loss. As the black hole attack may lead to the depletion of energy (battery power)of the nodes and the data inconsistency in the sensor network. False routing table information is generated by the attacker node during the formation of paths between the nodes in the network. The overall performance of the network is depleted if the black hole is present in the network.

In the proposed method, if the performance of the network is less than the threshold, then the node identifies the fake reply packet generated by the black hole and that black hole node is removed from the network and the network become secure. This enhances the network performance and reduces the battery utilization of the sensor nodes.

References:

[1] Ms. Snehal Deshmukh, Dr. S. S. Sonavane, "Security Protocols for the internet of Things:
A Survey",2017,978-1-5090-5913-3/17/$31.00_c 2017 IEEE. DOI:10.1109/ICNETS2.2017.8067900

[2] Mrs. Snehal Deshmukh-Bhosale, Dr. S. S. Sonavane, "Design of Intrusion Detection System for Wormhole Attack Detection in Internet of Things", Springer Nature Singapore Pte Ltd. 2020, Advanced Computing and Intelligent Engineering, Advances in Intelligent Systems and Computing 1082, https://doi.org/10.1007/978-981-15-1081-6_44

[3] Taylor Vincent F, Fokum Daniel T "Mitigating Black Hole Attacks in Wireless Sensor Networks Using Node-Resident Expert Systems", Washington, DC,pp.1-7,IEEE,2014.

[4] Mishra BinoodKumar,Nikam Mohan C,LakkadwalaPrashant," Security Against Black Hole attack in wireless Sensor Network –A Review",2014 Fourth International Conference on

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

communication System and Network Technologies, IEEE Computer Society Washington, DC, USA, pp.615-620, IEEE 2014.
[5] Wang Chun-Hsin and Li Yang-Tang, ―Active Black Holes Detection in Ad-Hoc Wireless Networks‖, Ubiquitous and Future Networks (ICUFN) 2013 Fifth International Conference on Da Nang, pp.94-99, IEEE, 2013.
[6] Mehdi Medadian, Ahmad Mebadi, ElhamShahri, ―Combat with Black Hole Attack in AODV Routing Protocol‖, Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications, 15 -17 December 2009, Kuala Lumpur Malaysia, IEEE 2009.
[7] Wazid Mohammad, KatalAvita, Goudar R H,"TBESP Algorithm for Wireless Sensor Network under BlackholeAttack",International conference on Communication and Signal Processing, April 3-5, 2013, India, pp.1086-1091, IEEE 2013.
[8] Samir Athmani, DjallelEddineBoubiche and AzeddineBilami,―Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs‖,Computer and Information Technology (WCCIT), 2013 World Congress on Sousse,pp.1-5,IEEE,2013.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731