Detection of black and grey hole attacks using TAODV scheme for WSN

Rajshekar G, Priyanka
Associate Professor, M.Tech Student, Research Scholar
Dept. of CSE, GNDEC, Bidar, Karnataka

Abstract: In mobile ad hoc networks (MANETs), a primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other. In the presence of malevolent nodes, this requirement may lead to serious security concerns; for instance, such nodes may disrupt the routing process. In this context, preventing or detecting malicious nodes launching grayhole or collaborative blackhole attacks is a challenge. This paper attempts to resolve this issue by designing a Trusted AODV-based routing mechanism that integrates the advantages of both proactive and reactive defense architectures. Our method implements a route tracing technique to help in achieving the stated goal to detect black hole attack, we also include the detection of gray hole attack which the Gray- Hole attack, malicious nodes try to stop the packets in the network by refusing to forward or drop the packets passing through them for considerable periods. Each intermediate node within the range.

Keywords: black hole detection, Attack detection.

1. INTRODUCTION

A Wireless Sensor Network (WSN) consists of hundreds or thousands of low cost nodes which could either have a fixed location or randomly deployed to monitor the environment. WSNs are a trend of the past few years, and they involve deploying a large number of small nodes. The nodes then sense environmental changes and report them to other nodes over flexible network architecture. Sensor nodes are great for deployment in hostile environments or over large geographical areas. Each sensor node has a separate sensing, processing, storage and communication unit. The position of sensor nodes need not be predetermined. This allows random deployment in inaccessible terrains or disaster relief operations. WSNs may be organized in a variety of different ways, and a solution designed for a flat network will unlikely is optimal for a clustered network. To be effective and efficient, a solution needs to be tailored to the particular network organization at hand. Due to their limited power and short range, sensor nodes need to collaboratively work in multi-hop wireless communication architectures to allow the transmission of their sensed and collected data to the nearest base station. Unlike wired networks where the physical wires prevent an attacker from compromising the security of the network, wireless sensor networks face many security challenges that represent a prerequisite to a successful deployment of wireless sensor networks especially for military applications. Moreover, the resource-starved nature of sensor nodes makes the security issue very critical; in fact, the deployment of maximum security services in each node will produce a significant drain on the system resources, and thus reduce the node’s lifetime. Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. A wireless sensor network (WSN) is a wireless network that consists of distributed sensor nodes that monitor specific physical or environmental events or phenomena, such as temperature, sound, vibration, pressure, or motion, at different locations. The first development of WSN was first motivated by military purposes in order to do battlefield surveillance. Nowadays, new technologies have reduced the size, cost and power of these sensor nodes besides the development of wireless interfaces making the WSN one of the hottest topics of wireless communication. There are four basic components in any WSN: (1) a group of distributed sensor nodes; (2) an interconnecting wireless network; (3) a gathering-information base station(Sink); (4) a set of computing devices at the base station (or beyond) to interpret and analyze the received data from the nodes.

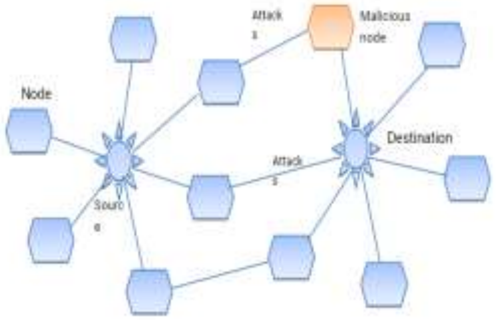
2. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before improving the tools it is compulsory to decide the economy strength, time factor. Once the programmer‘s create the structure tools as programmer require a lot of external support, this type of support can be done by senior programmers, from websites or from books.
H. Ma and D. Tao, For node awakening in wireless multi-sensor networks, an algorithm is put forward for three dimensional target tracking. To monitor target dynamically in three dimensional area by controlling nodes, we constract virtual force between moving target and the current sense node depending on the virtual potential method, then select the next sense node with information gain function, so that when target randomly move in the specific three dimensional area, the maximum sensing ratio of motion trajectory is get with few nodes. The proposed algorithm is verified from the simulations.

In this paper **H. Luo, Y. Liu, and S.K. Das** In sensor networks, en route aggregation decision regarding where and when aggregation shall be performed along the routes has been explicitly or implicitly studied extensively. However, existing solutions have omitted one key dimension in the optimization space, namely, the aggregation cost. In this paper, focusing on optimizing over both transmission and aggregation costs, we develop an online algorithm capable of dynamically adjusting the route structure when sensor nodes join or leave the network. Furthermore, by only performing such reconstructions locally and maximally preserving existing routing structure, we show that the online algorithm can be readily implemented in real networks in a distributed manner requiring only localized information. Analytically and experimentally, we show that the online algorithm promises extremely small performance deviation from the offline version, which has already been shown to outperform other routing schemes with static aggregation decision.

In this paper **M.P. Michaelides and C.G. Panayiotou** This paper investigates the use of wireless sensor networks for estimating the location of an event that emits a signal that propagates over a large region. In this context, we assume that the sensors make binary observations and report the event (positive observations) if the measured signal at their location is above a threshold; otherwise, they remain silent (negative observations). Based on the sensor binary beliefs, a likelihood matrix is constructed whose maximum value points to the event location. The main contribution of this work is Subtract on Negative Add on Positive (SNAP), an estimation algorithm that provides an efficient way of constructing the likelihood matrix by simply adding pm 1 contributions from the sensor nodes depending on their alarm state (positive or negative). This simple estimation procedure provides very accurate results and turns out to be fault tolerant even when a large percentage of the sensor nodes report erroneous observations.

3. SYSTEM ARCHITECTURE



1: System Architecture

In this architectural diagram, the nodes deployment along with the source, destination and attackers node. While attacks, the attackers may launch the types of attack to compromise the authentic node.

4. METHODOLOGY

Proper operation of MANET requires mutual cooperation of participating nodes. Due to presence of selfish or malicious nodes, performance of network degrades significantly. Selfish nodes drop packets coming from its neighbor nodes to conserve its energy or push forward their own packets in the buffer queue. To prevent this misbehavior, selfish nodes need to be detected and isolated from network.

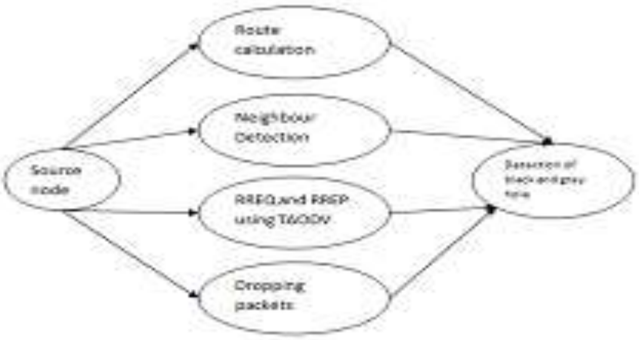


Figure 2: Use Case diagram

5. IMPLEMENTATION

Network simulator 2 is used as the simulation tool in this project. It has an open source code that can be modified and extended and is an object–oriented, discrete event simulator for networking and provides substantial support for simulation. It is written in C++, with an Otcl interpreter as a command and configuration interface. C++ is a compiled programming language needs to be compiled (i.e., translated) into the executable machine code where as Otcl is an interpreted programming language [11]. Upon execution, the interpreter translates Otcl instructions to machine code understandable to the operating system line by line.

To perform simulation and evaluate the performance following simulation parameters are used:

Simulator	NS2
Channel type	Channel/Wireless channel
Radio propagation n model	Propagation/Two ray ground
Network interface type	Phy/wireless Phy
MAC type	MAC/802_11
Interface queue type	Queue/Drop Tail/Pri Queue
Link layer type	LL
Antenna model	Antenna/Omni antenna
Max packet in ifq	300
Number of mobile nodes(nn)	50
Routing protocol	AODV
X dimension of topography	1670
Y dimension of topography	1200
Set opt initial energy	100

Table1: Parameters used

5. RESULTS AND DISCUSSION

We are using X-graph to evaluate the performance. We choose the following evaluation metrics.

- Throughput.
- Delay
- Overhead
- Packet delivery ratio(PDR)

The below table 2 show the parameters. The resulting graph is plotted.

Results

Parameters	Without malicious	With malicious
Throughput (kbps)	160.70	174.80
Delay(msec)	28.2001	83.20
PDR (%)	0. 9792	0. 98
Overhead(load)	2.922	3.106

Table 2: parameters for plotting graph

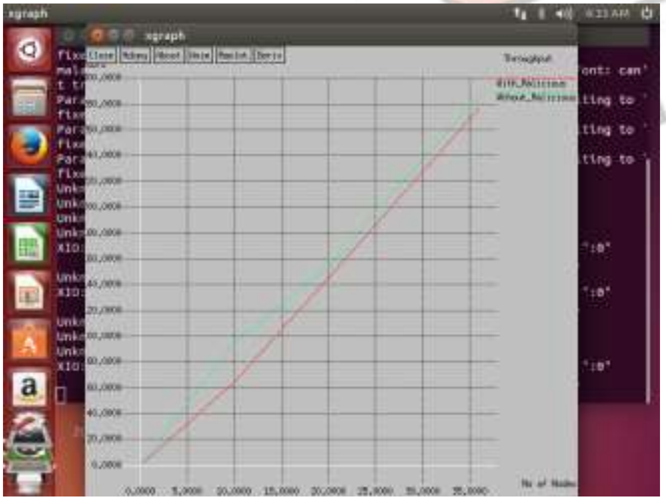


Figure 3: Throughput comparison Graph

The X-graph figure3 explains about throughput in terms of time more amounts of data is transferred i.e. throughput increases, 174 bits are transmitted in. This is one of the advantages of improving network throughput.

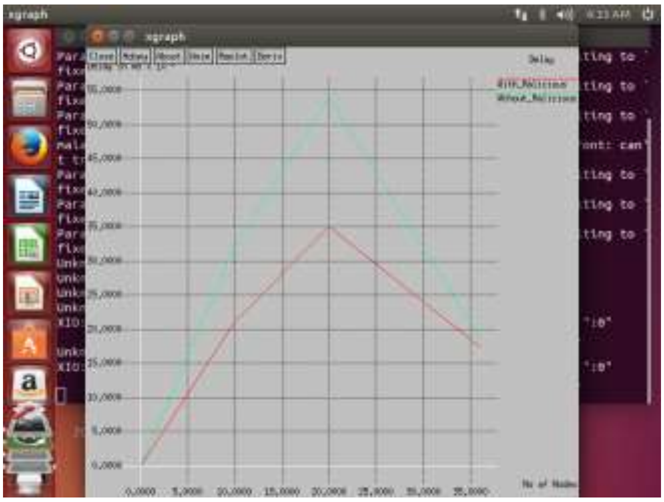


Figure 4: Average end to end delay graph

The above X-graph figure4 end to end delay is calculated using difference in sent and received time, measured in mili seconds or micro seconds. Includes all possible delays caused by buffering during route discovery at queuing significant in understanding the delay introduced by path discovery.

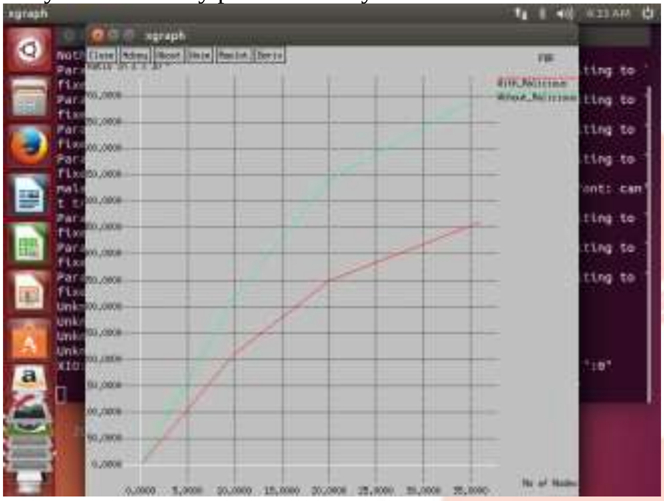


Figure 5: Packet delivery ratio (PDR) comparison graph

The above X-graph figure5 shows PDR for total packet sent by total packet received, measured in percentage (%). Represents value for packet delivery ratio. The number of packets transmitted by source and the number of packets acknowledge by destination.

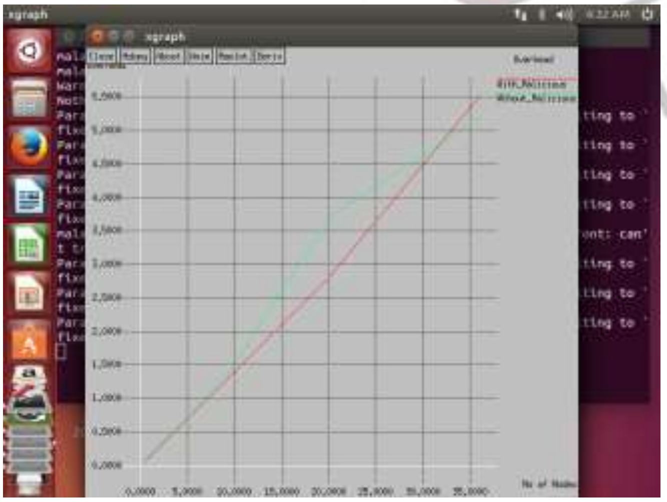


Figure 6: Overhead comparison graph

The above X- graph in figure6 shows that it is number of packet processed, measured in terms of load.

CONCLUSION

This approach help in detecting blackhole attack in network with the help of TAODV RREQ scheme, results has been analyzed with the help of PDR, throughput and delay metrics, in future work can be extended by deploying more than one base node in network, so in case of failure of one base node, network continue to detect blackhole and further network can be analyzed with the help of metrics like Jitter, Routing overhead, energy etc. Proposed energy efficient technique encloses a feasible trust based solution to detect Gray-Hole and Black-Hole attacks in WSNs and generate a secure routing path from source to the sink node. The algorithm is implemented to prevent the compromised node to selection mechanism that significantly improves the network performance with respect to packet drop ratio, end-to-end delay.

FUTURE ENHANCEMENTS

The research work implemented in this paper can be extended further to modify the proposed algorithm to increase the communication among sensors and hence to reduce network bandwidth consumption in the whole WSNs and also for to provide security over packet transmission along with increase in energy efficiency in WSNs.

ACKNOWLEDGMENT

We indebted to management of GNDEC, Bidar for excellent support in completing this work at right time. A special thanks to the authors mentioned in the references.

REFERENCES

[1] Gurung, Shashi, and Krishan Kumar Saluja. "Mitigating Impact of Blackhole Attack in MANET." Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC. 2014.

[2] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." Humancentric Computing and Information Sciences 1.1 (2011)

[3] Vu, Cong Hoan, and Adeyinka Soneye. An Analysis of Collaborative Attacks on Mobile Ad hoc Networks. Diss. Master Thesis at School of Computing, Blekinge Institute of Technology, 2009.

[4]Dhurandher, Sanjay Kumar, et al. "GAODV: A Modified AODV against single and collaborative Black Hole attack inMANETs. " Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on. IEEE, 2013..

[5] J.Sen, S. Koilakonda, A. Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Adhoc Networks" IEEE Second International Conference on Intelligent Systems, Modeling and Simulation, 2011.

[6] Bindra, Gundeep Singh, et al. "Detection and removal of co-operative blackhole and grayhole attacks in MANETs." System Engineering and Technology (ICSET), 2012 International Conference on. IEEE, 2012.

[7] Hiremani, Vani, and Manisha Madhukar Jadhao. "Eliminating co-operative blackhole and grayhole attacks using modified EDRI table in MANET."Green Computing, Communication and Conservation of Energy (ICGCE), 2013 International Conference on. IEEE, 2013.

[8]Wahane, Gayatri, and Savita Lonare. "Technique for detection of cooperative black hole attack in MANET." Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. IEEE, 2013.

[9] Biswas, Santosh, Tanumoy Nag, and Sarmistha Neogy. "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET." Applications and Innovations in Mobile Computing (AIMoC), 2014. IEEE, 2014.

[10] Nishu kalia, Kundan Munjal, "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol" International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2, Issue-3, February 2013.