IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907164 |

The Trust Computation model for Secure Network Monitoring in WSN

Chinmay Kulkarni, Dr D. N. Patil

PG Student, Department of Computer Engineering, Sinhgad College of Engineering, Pune, India

Professor: Department of Computer Engineering, Sinhgad College of Engineering, Pune, India

ABSTRACT : Wireless Sensor Networks (WSNs) because of their resource-constrained characteristics increasingly being deployed as they are prone to security attacks like black hole attack and more. WSN has wide range of applications such as traffic surveillance, flood detection, battlefield surveillance etc. and also it obstructs normal operation of network as has potential to suspect various attacks. This paper presents a footstep on developing a network monitoring tool for monitoring network devices and hosts. Using a combination of Simple Network Monitoring Protocol (SNMP), Internet Control Message Protocol (ICMP) and port scanning concept a software based network monitoring tool is being developed. As WSN become wide spread, security becomes a cardinal affair. One of the terrible threats is Denial of Service (DoS) that not only affects the network bandwidth but also affects the performance of the network. Data collection can also be affected in WSN because of Dos and Black hole attacks. This paper use a system named as Active trust system that effectively detect and prevent both DoS and Black hole attack. In this system, two protocols are used such as: Active detection routing protocol that acutely detects attackeras behaviour and location and Active trust route protocol that created define detection routes with low energy consumption. Also for attack prevention, system makes use of SHA1 hashing algorithm in which only previous node hash data is send to next node. In this way, proposed system successfully detects and prevents the DoS and Black hole attack by enhancing network lifetime and low energy consumption with high security.

KEYWORDS: Attack detection and prevention, Black hole attack, Dos attack, Hashing, ICMP, Security, SNMP, WSN.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are emerging as a promising technology because of their wide range of applications in industrial, environmental monitoring, military and civilian domains. Due to economic considerations, the nodes are usually simple and low cost. They are often unattended, however, and are hence likely to suffer from different types of novel attacks. A black hole attack is one of the most typical attacks and works as follows. The adversary compromises a node and drops all packets that are routed via this node, resulting in sensitive data being discarded or unable to be forwarded to the sink. Because the network makes decisions depending on the nodesEa sensed data, the ¨ consequence is that the network will completely fail and, more seriously, make incorrect decisions. Therefore, how to detect and avoid black hole attack is of great significance for security in WSNs.

A Wireless Sensor Network (WSN) is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc. WSNs are regarded as a revolutionary information gathering method to build the information and communication system which will greatly improve the reliability and efficiency of infrastructure systems. Compared with the wired solution, WSNs feature easier deployment and better flexibility of devices. With the rapid technological development of sensors, WSNs will become the key technology for IoT. The security in Wireless Sensor Networks (WSNs) is a critical issue due to the inherent limitations of computational capacity and power usage. While a variety of security techniques are being developed and a lot of research is going on in security field at a brisk pace but the field lacks a common integrated platform which provides a comprehensive comparison of the seemingly disconnected but linked issue user we attemptto comparative analysis of the various available security approaches highlighting their advantages and weaknesses. This paper consider routing security in Wireless Sensor Networks. Many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal and propose security goals for routing in sensor networks.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907164 |

Network monitoring tool monitors all the network belongings like switches, routers and firewall. There is much study available on monitoring network and network devices as well. Some network monitoring tools like Nagios, Shinken do provide network monitoring but has certain limitations as they are not able to provide end-to-end packet delivery from source to destination. The proposed system is overcoming this drawback of existing tools as it provides end-to-end packet delivery from source to destination. Also existing systems has limitations to attacks as they are not secure. Attacks like Black Hole and Denial of Service are prior in networks. Although there is much research on black hole attacks and DoS attacks. Such studies mainly focus on the strategy of avoiding these attacks. Another approach does not require black hole information in advance. In this approach, the packet is divided into M shares, which are sent to the sink via different routes (multipath), but the packet can be resumed with T shares (T ¡= M). However, a deficiency is that the sink may receive more than the required T shares, thus leading to high energy consumption. Another preferred strategy that can improve route success probability is the trust route strategy. The main feature is to create a route by selecting nodes with high trust because such nodes have a higher probability of routing successfully; thus, routes created in this manner can forward data to the sink with a higher success probability.

II. LITERATURE SURVEY

The main purpose of study reviewed to focus on the secure and trustable routing protocol in Wireless Sensor Networks. Focus on the existing methods or protocol to make WSN secure and trustable. Studied how researchers try to solve the security and trust related issues. Also discuss the existing methodologies advantages, disadvantages and limitations and overcome the existing problem.Single-path routing is a simple routing protocol but is easily blocked by the attacker. Therefore, the most natural approach is via multi-path routing to the sink. Even if there is an attack in some route, the data can still safely reach the sink. Multi-path routing protocols can be classified into two classes depending on whether the data packet is divided. One is multi-path routing without share division. The other is multi-path routing with share division, i.e., the packet is divided into shares, and different shares reach the destination via different routes. Non-share-based multi-path routing. There are different multi-path route construction methods. Ref. proposes a multi dataflow topologies (MDT) approach to resist the selective forwarding attack. In the MDT approach, the network is divided into two dataflow topologies. Even if one topology has a malicious node, the sink can still obtain packets from the other topology. In such protocols, the deficiency is that if the packet is routed via n routes simultaneously, the energy consumption will be n times that of a single path route, which will seriously affect the network lifetime; similar research can be seen in multi-path DSR , the AOMDV and AODMV

Wireless Sensor Networks (WSNs) are increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection. To conquer that challenge, an active detection-based security and trust routing scheme named ActiveTrust is proposed [1] for WSNs. The most important innovation of ActiveTrust is that it avoids black holes through the active creation of a number of detection routes to quickly detect and obtain nodal trust and thus improve the data route security. This paper [2] proposes a highly Scalable Monitoring Tool for Wi-Fi networks which is based on existing wi-fi hotspot concept. Using syslog protocol data collection and visualization of network components is done. This paper [3] examines Fair Routing in Overlapped Cooperative Heterogeneous Wireless Sensor Networks which mainly focuses on lifetime of network components. Focuses on heterogeneous characters like battery capacity, number of nodes, energy consumption, nodes locations, packet transmission time etc. to improve performance ofnetwork based on heterogeneous overlapped WSNs. This paper [4] proposes a Multi-Metric energy efficient routing in mobile ad-hoc networks as consumption of energy across the network is major concern while routing the data packets. This paper proposes the multi-metric system using MAC queue concept for sending packets from source to destination using by consuming less energy. This paper [5] Spatial Reusability-Aware Routing in Multi-Hop Wireless Networks which tends to achieve high end-to-end throughput. Based on Spatial Reusability-Aware Singlepath Routing (SASR) and Anypath Routing (SAAR) cost optimization is done to select best route in multi hop wireless network.

This paper [6] presents the position-aware, secure, and efficient mesh routing approach (PASER). Their proposal prevents more attacks than the IEEE 802.11s/i security mechanisms and the well-known, secure routing protocol ARAN, without making restrictive assumptions. In realistic UAV-WMN scenarios, PASER achieves similar performance results as the well-established, non-secure routing protocol HWMP combined with the IEEE 802.11s security mechanisms. In this paper [7], Ren et al. propose an analytic model to estimate the entire network lifetime from network initialization until it is completely

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907164 |

disabled, and determine the boundary of energy hole in a data-gathering WSN. Specifically, they theoretically estimate the traffic load, energy consumption, and lifetime of sensor nodes during the entire network lifetime. Furthermore, they investigate the temporal and spatial evolution of energy hole and apply their analytical results to WSN routing in order to balance the energy consumption and improve the network lifetime. In a heterogeneous environment, naive lifetime improvement with cooperation may not be fair. In this paper [8], Kinoshita et al. propose a fair cooperative routing method for heterogeneous overlapped WSNs. It introduces an energy pool to maintain the total amount of energy consumption by cooperative forwarding. The energy pool plays a role of broker for fair cooperation. Sinhgad College of Engineering, Pu

III. PROPOSED SYSTEM DESIGN

Proposed an active detection-based security and trust routing scheme ActiveTrust to overcome the challenges of various security attacks and a black hole attack, DoS attack which affects data collection seriously in WSNs.The ActiveTrust scheme is the first routing scheme that uses active detection routing. The most significant difference between Active Trust and previous research is that we create multiple detection routes in regions with residue energy; because the attacker is not aware of detection routes, it will attack these routes and, in so doing, be exposed. In this way, the attackerEasbehavior and location, as well as nodal trust, can be obtained ¨ and used to avoid black holes when processing real data routes. To the best of our knowledge, this is the first proposed active detection mechanism in WSNs. The Active Trust route protocol has better energy efficiency. Energy is very precious in WSNs, and there will be more energy consumption if active detection is processed. Therefore, in previous research, it was impossible to imagine adopting such high-energy-consumption active detection routes. However, we find it possible after carefully analyzing the energy consumption in WSNs. Research has noted that there is still up to 90% residue energy in WSNs when the network has died due to the aenergy hole ˆ a phenomenon. Therefore, the ˆ Active Trust scheme takes full advantage of the residue energy to create detection routes and attempts to decrease energy consumption in hotspots (to improve network lifetime). Those detection routes can detect the nodal trust without decreasing lifetime and thus improve the network security.Proposed System An overview of the ActiveTrust scheme, which is composed of an active detection routing protocol and data routing protocol, is shown in Figure 1.

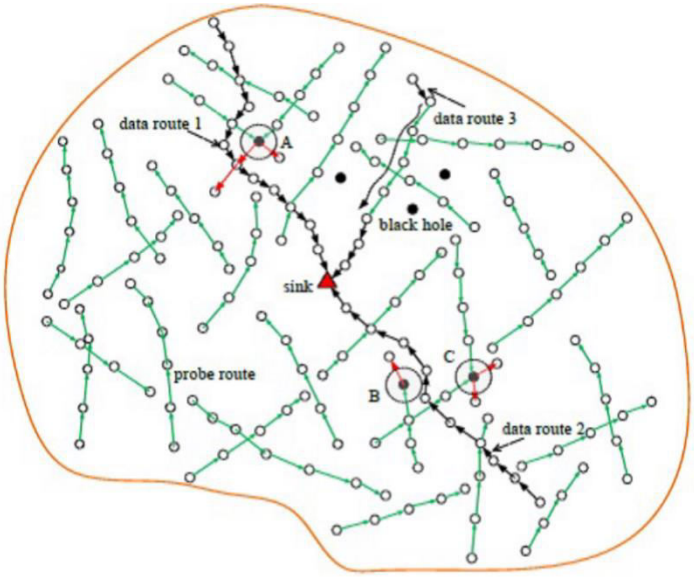

Figure 1: proposed active trust Scheme

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907164 |

Algorithm Design

Algorithm 1: Active Detection Routing Protocol

1. Initialization

2. for each neighbor node An Do

3. Let An.accesTime = Currenttime

4. End for

5. For each node that generates a detection packet, such as node A, Do

6. Construct packet P, and do value assignment for ω and $

7. Select B as the next hop which B meets access time is the minimum and nearer the sink //B is the node that is the longest time undetected and nearer the sink

8. Send packet P to node B

9. End for

10. For each node that receives a detection packet, such as node B, Do

11. Let P.ω = P. ω - 1; P $ = P. $ - 1

12. If $ = 0 then

13. Construct feedback packet q, and do value assignment for each part

14. Send feedback packet q to the source

15. End if

16. If P.ω 6= 0 then

17. Detection routing continue

18. End if

19. End for

20. For each node that receives feedback packet q, such as node C, Do

21. If q.destination is not itself then

22. Send q to the source node

23. End if

24. End for

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907164 |

Algorithm 2: Data Routing Protocol

1. For each node that generates or receives a data packet, such as node A, Do

2. Select B as the next hop such that B has never been selected in this data routing

process, has the largest trust and is nearer the sink

3. If A finds such node, for instance, node B

4. Send data packet P to node B

5. If node B is the sink then

6. this data routing procession is completed

7. End if

8. Else

9. Send failure feedback to the upper node, such as node C

10. End if

11. End for

12. For each node that receives failure feedback, such as node B, Do

13. Repeat step 2 to step 11

14. End for

Mathematical Model

End-to-end Encoding: At every generation of new confidential message, i.e., Let , Ps(t)=0, let ks(t+1)=ks(t)+1,and determine end-to-end confidential encoding rate.

Flow control: At each block, for some, each source injects confidential bits into its queues:

Encoding:-

Encoding of each letter in secret message by its equivalent ASCII code

1. Conversion of ASCII code to equivalent 8 bit binary number.

2. Division of 8 bit binary number into two 4 bit parts.

3. Choose of suitable letters corresponding to the 4 bit parts.

4. Meaningful sentence construction by using letters obtained as the first letters of suitable words.

5. Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction.

6. Encoding is not case sensitive.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907164 |

Decoding

1. First letter in each word of cover message is taken and represented by corresponding 4 bit number.

2. 4 bit binary numbers of combined to obtain 8 bit number.

3. ASCII codes are obtained from 8 bit numbers.

4. Finally, secret message is recovered from ASCII codes.

Let us consider S as a set confidential Wireless Sensor Networks with effective key management…

S= { }

Identify the inputs as number of nodes

F= {f1, f2, f3 ....., fn} 'F' as set of functions to execute to routing model}

I= {i1, i2, i3…|'I' sets of inputs to number of nodes/ sensors}

O= {o1, o2, o3….|'O' Set of outputs from the function sets}

S= {I, F, O}

I = {Number of nodes}

O = {Shortest routing path for multi hop protocol}

F = {AODV, ARQ,, Euclidean distance, Pair wise key}

IV. RESULTS AND DISCUSSION

In this section we present the evaluation of proposed system as well as existing system. After describing our experimental setup, we quantitatively evaluate the analysis with respect to the different parameter used such as throughput, packet delivery ratio, cost, and time. We run our experiments in NS2 simulator version 2.35 that has shown to produce realistic results. NS simulator runs TCL code, but here use both TCL and C++ code for header input. In our simulations, we use Infrastructure based network environment for communication. For providing access to the wireless network at anytime used for the network selection. WMN simulate in NS2 .TCL file show the simulation of all over architecture which proposed. For run .TCL use EvalVid Framework in NS2 simulator it also help to store running connection information message using connection pattern file us1. NS2 trace file .tr can help to analyze results. It supports filtering, processing and displaying vector and scalar data. The results directory in the project folder contains us.tr file which is the files that store the performance results of the simulation. Based on the us.tr file using xgraph tool we execute graph of result parameters with respect to x and y axis parameters. Graphs files are of .awk extensions and are executable in xgarph tool to plot the graph. Introduction=fter studying various tools for simulation, I found that the network simulator (ns2) can be used as a simulator for the proposed system because we can use Bluetooth and Wi-Fi and we can follow our conditions.The simulation parameters has used which is described in below table

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907164 |

Table 1 : Parameters and Values

Parameter	Values
Simulator	NS-allinone 2.35
Simulation time	25 Seconds
Channel-Type	Wire-less Channel
Propagation-Model	2 Ray Ground
Standard	MAC/802.11
Simulation Size	1000 *1500
Max packet Length	1000
Ad hoc routing	AODV, SAODV, DSR, DSDV
Traffic	CBR, PBR

Performance Metrics and parameters

Throughput

It is defined as the ratio of the total number of bits received by the destination to the total simulation time. The throughput is a function of the mobility pattern, if two nodes are always adjacent and move together, the throughput for the TCP connection between them would be identical to that for 1 hop. On the other hand, if the two nodes are always in different partitions of the network, throughput is 0. Improved congestion avoidance for TCP vegas is implemented using TCL script. Execution of tcl script generates a trace file with all simulation events recorded in it. Throughput is calculated using awkscript which process the trace file and produces the results in a file. Throughput is plotted using results obtained from execution of awk script is as shown in figure 2.

The below figure demonstrates Throughput with four different protocol in watchdog and proposed system, it slightly improve the throughput values using DSR in simulation.

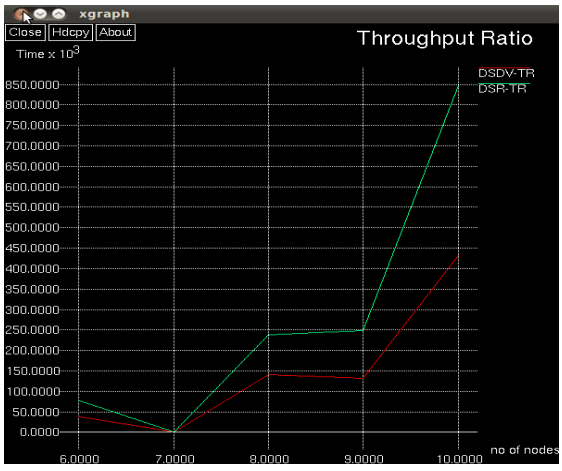

Figure 2 : Simulation results for No. of nodes vs Throughput

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907164 |

End to End Delay

It is defined as the time taken for a packet to be transmitted across network from source to destination. The lower the delay the better is the performance. high channel delays in a mobile network causing the TCP timer to expire will force TCP to unnecessarily retransmit the delayed packet and to consume more time and energy resulting in network performance degradation.As shown in figure 3, the demonstrates result graph shows this variation of delay defined on y axis with respect to no. of nodes defined on x axis and it is observed that delay is not stable with respect to nodes because of incompleteness of environmental awareness. Also, it is observed that delay for proposed with DSR is less than DSDV.

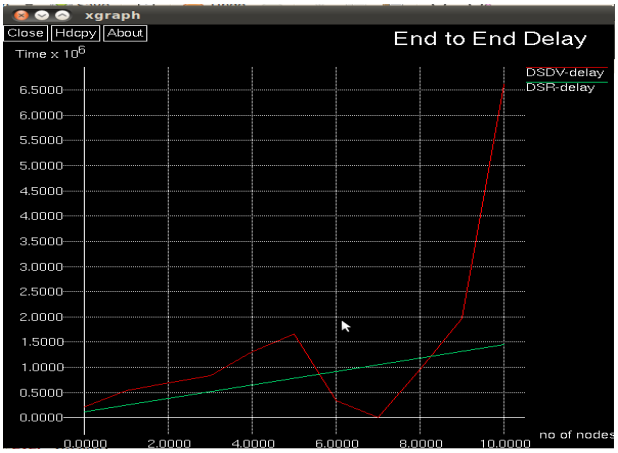

Figure 3 :Simulation results for No. of nodes vs Delay

Control Overhead

Overhead is any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to attain a particular goal. Routing overhead affects the amount of time used for sending and receiving the routing packets, the chosen routes affect which nodes will have faster decrease in energy. For very dynamic topologies, proactive protocols can introduce a large overhead in bandwidth and energy consumption on the network. Reactive protocols trades off this overhead with increased delay, as the route to the destination is established when it is needed based on an initial discovery between the source and the destination. As shown in figure 3, the simulation graph indicates the variation of Control overhead(y axis) with respect to no. of nodes (x axis) and it is observed that control overhead of DSR less as compare to DSDV. Control overhead of Proposed DSR increases as no. of nodes increases.

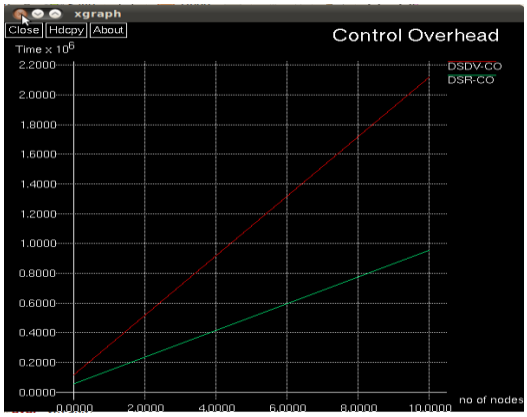

Figure 4 : Simulation results for No. of nodes vs Control overhead

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907164 |

Packet Delivery Ratio

It is defined as the ratio of the total number of packets received by the destination node to the number of packets send by the source node. The simulation graph indicates the variation of Packet Delivery Ratio(y axis) with respect to no. of nodes (x axis) and it is observed that PDR of DSR is high as compare to DSDV Proposed protocol which is as shown in figure 5.

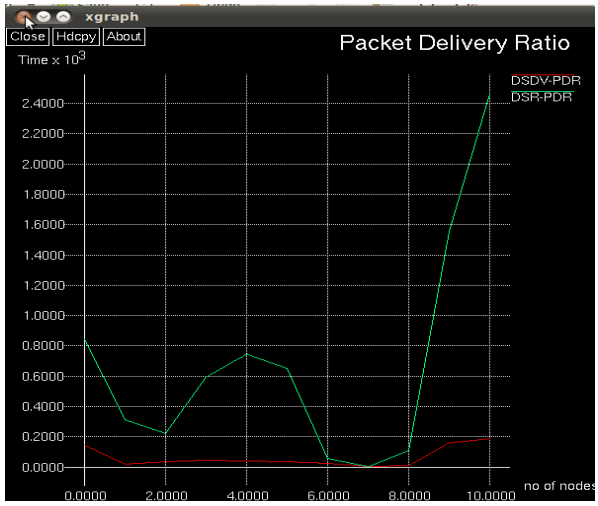

Figure 5 : Simulation results for No. of nodes vs Packet Delivery Ratio

Packet Drop Ratio

It is defined as the ratio of the total number of packets drop by the destination node to the number of packets send by the source node. The simulation graph indicates the variation of Packet Drop Ratio (y axis) with respect to no. of nodes (x axis) and it is observed that packet drop rate of DSR is less than compare to DSDV Proposed protocol which is as shown in figure 8.5.

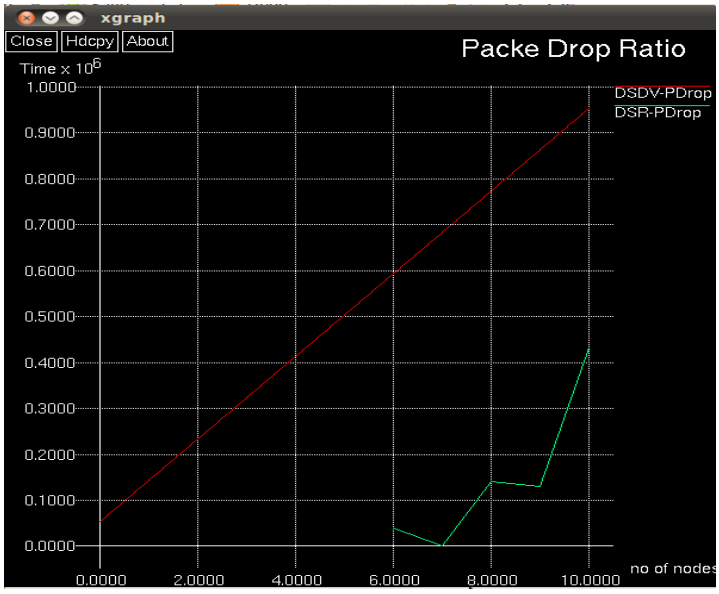

Figure 5 : Simulation results for No. of nodes vs Packet Delivery Ratio

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907164 |

V. CONCLUSION

This paper proposed a novel security and trust routing scheme based on active detection which effectively detect and prevent both DoS and Black hole attack. In this framework, two protocols are utilized, which are Active detection routing protocol that intensely detects attacker's behavior and location and Active trust route protocol that made detection routes with low energy utilization. Likewise for attack prevention, framework makes utilization of SHA1 hashing algorithm in which only previous node hash data is send to next node. The proposed framework effectively recognizes and prevents the DoS and Black hole attack by low energy utilization with high security and enhanced network lifetime.

REFERENCES

[1] Yuxin Liu, Mianxiong Dong, Kaoru Ota, Anfeng Liu, "ActiveTrust: Secure and Trustable Routing inWireless Sensor Networks", IEEE Transactions on Information Forensics and Security, 1556-6013 (c) 2016.
[2] Machaka, P., Bagula, A. and DeWet, "A Highly Scalable Monitoring Tool forWi-Fi Networks", ISAT 2015.
[3] EvripidisParaskevas, KyriakosManousakisy, SubirDasy and John S. Baras, "'Multi-Metric Energy Efficient Routing in Mobile Ad-Hoc Networks"', arXiv:1603.09386v1, Mar 2016
[4] Kazuhiko Kinoshita, Natsuki Inoue, Yosuke Tanigawa, Hideki Tode and Takashi Watanabe, "Fair Routing for Overlapped Cooperative Heterogeneous Wireless Sensor Networks", IEEE Sensors Journal, Vol. 16, No. 10, May 15, 2016.
[5] Tong Meng, FanWu, Zheng Yang, Guihai Chen, "'Spatial Reusability-Aware Routing in Multi-Hop Wireless Networks"', IEEE Transactions on Computers, Vol. 65, No.1, Jan 2016.
[6] Tseng-Yi Chen, Yuan-Hao Chang, Ming-Chang Yang, Yun-Jhu Chen, Hsin-Wen Wei, andWei-Kuan Shih, "Multi-Grained Block Management to Enhance the Space Utilization of File Systems on PCM Storages", IEEE Transactions on Computers, Vol. 65, No. 6, June 2016.
[7] Wen-HsingKuo and Yung-Hsuan Lin, "Resource-Saving File Management Scheme for Online Video Provisioning on Content Delivery Networks", IEEE Transactions on Computers, Vol. 65, No. 6, June 2016.
[8] MohamadSbeiti, NiklasGoddemeier, Daniel Behnke, Christian Wietfeld, "'PASER: Secure and Efficient Routing Approach"', IEEE transactions on Wireless Communications, Vol. 15, No. 3, Mar 2016.
[9] MohamadSbeiti, NiklasGoddemeier, Daniel Behnke and Christian Wietfeld, "PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks", IEEE Transactions on Wireless Communications, Vol. 15, No. 3, March 2016.
[10] JuRen, Yaoxue Zhang, Kuan Zhang, Anfeng Liu, Jianer Chen, and Xuemin (Sherman) Shen, "Lifetime and Energy Hole Evolution Analysis in Data-GatheringWireless Sensor Networks", IEEE Transactions on Industrial Informatics, Vol. 12, No. 2, April 2016.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details