CRYPTO MARK SCHEME FOR FAST POLLUTION DETECTION AND RESISTANCE OVER NETWORKING

G.S.Pugalendhi[1]

[1] *Assistant Professor, Department of Computer science and Engineering, V.S.B Engineering College, Karur, Tamilnadu India*

---***---

Abstract : **Data security and data protection against pollution attacks with resource efficiency are the major challenging tasks of networks. Packet dropping and modifications are also common attacks that can be launched by an adversary to disrupt communication in networks. Many schemes have been proposed to mitigate, prevent those attacks. But very few can efficiently identify the pollution attackers with the delay and cost considerations. Even those schemes could find after the attacks done. Those type of schemes used packet HOP_VOTE techniques to investigate and verify the security issue .To address these issues, the proposed system introduces a simple and powerful scheme. The scheme which is a rapid identifier of polluters and this helps to identify misbehaved data and routes that dropped or modified packets. And this proposed system also considers the other type of security issues such as pollution attacks, packet content modification and packet dropping attacks. In order to identify and prevent the data from unauthorized forwarders, the system proposed a new scheme which is named as HOPVOTE The proposed system utilizes the HOPVOTE which is an efficient packet HOPVOTE technique to protect, prevent and avoid routing misbehaving attacks. In order to identify and block the nodes which tries to drop or modify the data, the proposed system has been implemented the Keybit verification algorithm. The proposed system also recovers the data which are polluted and retransmits using cache based recovery concept. The procedure behind the proposed system is to identify the key and its value of every packet with secured data transmission.**

Keywords *-HOPVOTE; OLSR; TAG_ENCODE_DECODE key; MARK mechanism*

1. INTRODUCTION

Networking is the word basically relating to computers and their Connectivity. It is often used in world of computers and their use in different connections. The term networking implies the link between two or more computers and their devices with a vital purpose of sharing data stored in the computers with each other. Organizations of different structures sizes and budgets need different types of networks. It can be divided into two categories:

1.1 Peer to Peer network:

A peer to peer network has no dedicated servers instead a number of workstations are connected together for the purpose of sharing information or devices. It is designed to satisfy the networking needs of home networks of small companies that do not want to spend a lot of money on a dedicated server. But still want to have the capability to share information or devices like in school, college, cyber café [2] [3].

1.2 Server based networks:

In server based network data files that will be used by all of the users are stored on the one server. This will help by giving you a central point to set up missions on the data files [1]. After compromising one or multiple nodes, an adversary may launch various attacks to disrupt the in-network communication. The attacks are commonly divided into two common problems, which are dropping packets and modifying Packets. Packets should not be filtered out while traveling because they should be used as evidence to infer packet modifiers [4]. So it cannot be used together with existing packet filtering schemes this is a major problem of existing system. To deal with packet droppers and polluters a widely adopted countermeasure is used, which is multipath forwarding in that each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated. Inherent weakness of network coding is that it is particularly vulnerable to pollution attacks. Malicious nodes can inject corrupted packets into a network, which get combined and forwarded by downstream nodes, thus causing a large number of corrupted packets propagating in the network [2] [6].

2. PROPOSED SCHEME

This module implements the novel HOP_VOTE scheme along with tag based authentication scheme for effective pollution attack detection, recovery and blocking. This allows a node to verify if it received packets belong to specific rule criteria, even if the encrypted key is expanding over time. Based on the id and tag creation the data will be routed. The packet filtering mechanism comes under Enhanced Scheme. This combines the basic schemes which are tag verification and a packet filtering mechanism to tolerate, find and eliminate packet polluters over the network. In this scheme the sender attaches a single bit of encrypted key in each packet with is named as HOP_Vote. The authentication key is unique to the packet and cannot be polluted anymore. Pollution attack is reduced [11] [10][9].

- Attacker is identified at once attack is made.
- Abnormal packet size is reduced using hopvote scheme.
- Prevention over packet content modification and packet dropping attacks.

2.1 Feasibility Study

A system is a feasible system only if it is feasible within limited resource and time. In this system each and every process can be feasible for the user and also developer. It proved user friendly input such as device independent inputs and getting proper solution for the problem [8].

2.2 Technical Feasibility

Technical Feasibility is the assessment of the technical view of the system. The system is developed for JAVA environment a platform independent tool is used to develop the system. The development risk concerns the probability, the function of all elements and its performance should be same in all platforms and in the system that is being developed. This system is developed according to the standards and the development software tools are selected to avoid the problems cited above [4] [7].The software used to develop this system is Windows XP, visual studio dot net is done efficiently, and the concept of SQL helps to create the application back end. These components are also helpful in providing interactivity to Java applications.

2.3 Behavioral Feasibility

It is common knowledge that computers illustrations have something to do with turnover transfers, retraining and changes in user or developer status. The main emphasis is customer service, personal contacts with customers Feasibility report is directed towards management. It evaluates the impact of the proposed changes on the area in question. The report is a formal document for management use, brief enough and sufficiently non-technical to be understood [6].

2.4 Economic Feasibility

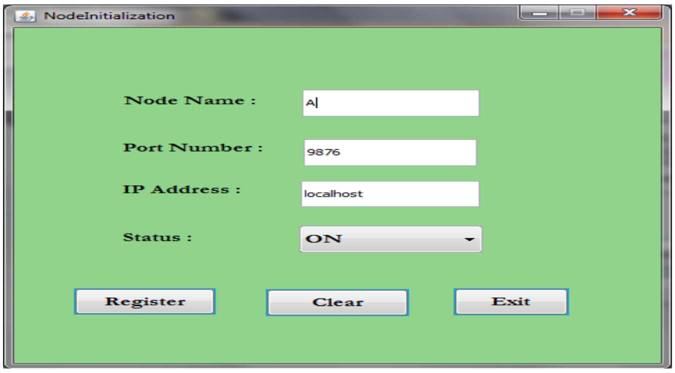
Economic feasibility or cost benefit is an assessment of the economic justification for a computer based system project. Though this system the administrator can use the tool from anywhere within their concern. The system is developed using the existing resources [9] [8]. So the project is economically feasible. This is the most frequently used method for evaluating the effectiveness of a user system. More commonly, known as cost analysis the procedure is to determine the benefits and savings that are expected from a candidate system and compare them with costs.

2.5 Operational Feasibility:

Operational Feasibility deals with the study of prospects of the system. These systems operationally eliminate all the tensions of the administrator and helps in effectively tracking the project progress [5]. This kind of automation will surely reduce the time and energy, which previously consumed in manual work. Based on the study, the system proved to be operationally feasible.

3. NETWORK STRUCTURE ANALYSIS

Client-server computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await (listen to) incoming requests. The parameters to construct a network are, the node name is nothing but the system name, which can be given by the user. The next value is host number which can be getting from our network configuration details. The next one is the IP address of the system. These can be identified by a simple command on DOS environment. The command, net stat helps to get all details about the network configuration.


NodeInitialization

Node Name : A

Port Number : 9876

IP Address : localhost

Status : ON

Fig-1: Node Initialization

3.1 Topology Construction:

Here it uses mesh topology because of its unstructured nature. Topology is constructed by getting the names of the nodes and the connections among the nodes as input from the user. While getting each of the nodes, their associated port and IP address is also obtained. For successive nodes, the node to which it should be connected is also accepted from the user. While adding nodes, comparison will be done so that there would be no node duplication. Then we identify the source and the destinations. The node information consists of node names and the weight between them.

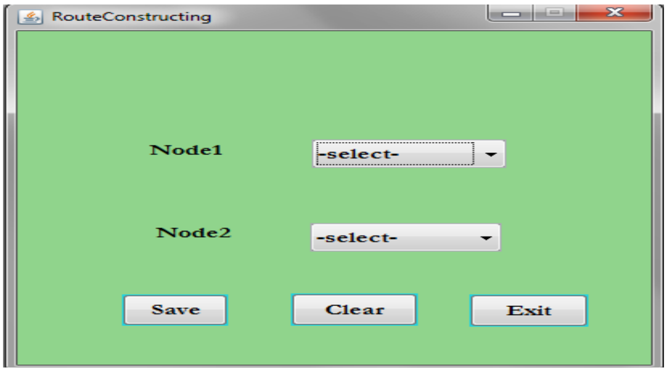


Fig-2: Topology Construction

3.2 Routing Protocol (OLSR)

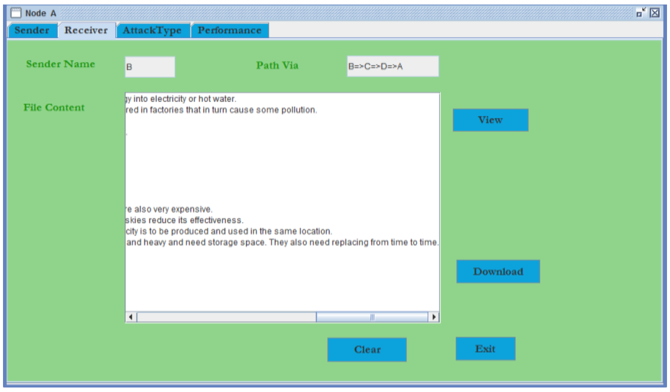
This module implements the novel OLSR message authentication code. Link-state routing protocols such as Open Shortest Path First (OSPF) and ISI Select a *designated router* on every link to perform flooding of topology information. In wireless networks, there is different notion of a link, packets can and do go out the same interface; hence, a different approach is needed in order to optimize the flooding process. Using Hello messages the OLSR protocol a teach node discovers 2-hop neighbor information and performs a distribute detection of a set of *multipoint relays* (MPRs). Nodes select MPRs such that there exists a path to each of its 2-hop neighbors via a node selected as an MPR.

3.3 Message Transmission:

In this module we transmit the message from source to destination. Here choose a destination and select a number of intermediate for that destination. Tag creation and path is calculated by TAG_ENCODE_DECODE mechanism. It will take minimum node cost an account to find the path between a source and destination. The HOP_VOTE key is updated in packet frequently. The source obtains the keys from the packet and compares. After receiving a message the destination will send an acknowledgement to the corresponding source.

3.4 Preventing pollution

HOP_VOTE scheme is introduced in the network to identify the data attacker nodes. To give data freshness the TAG_ENCODE_DECODE key is verified in the every hop node. Whenever the nodes act as a polluter in the next that node is identified and it is reported to the server node.



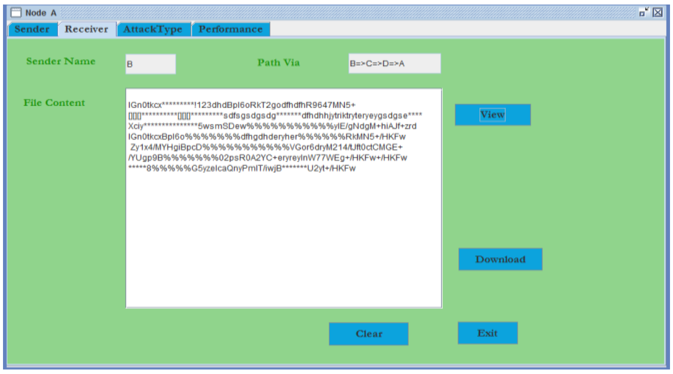
Sender Name B
Path Via B=>C=>D=>A
File Content

```
)y into electricity or hot water.
red in factories that in turn cause some pollution.



e also very expensive.
skies reduce its effectiveness.
city is to be produced and used in the same location.
 and heavy and need storage space. They also need replacing from time to time.
```

Fig-3: Transmission without Attack



Sender Name B
Path Via B=>C=>D=>A
File Content

```
IGn0tkcx*********!123dhdBpl6oRkT2godfhdfhR9647MN5+
[][][]**********[][][]*********sdfsgsdgsdg*******dfhdhhjytriktryteryeygsdgse****
Xciy***************5wsmSDew%%%%%%%%%%%ylE/gNdgM+hiAJf+zrd
IGn0tkcxBpl6o%%%%%%%dfhgdhderyher%%%%%%RkMN5+/HKFw
 Zy1x4/MYHgiBpcD%%%%%%%%%%%VGor6dryM214/tJft0ctCMGE+
/YUgp9B%%%%%%02psR0A2YC+eryreylnW77WEg+/HKFw+/HKFw
*****8%%%%%G5yzelcaQnyPmlT/iwjB*******U2yt+/HKFw
```

Fig-4: Transmission with Attack

4. SIMULATION RESULTS

System implementation is the stage where the theoretical design turned into the working system. The most crucial stage the user confidence the new system will work efficiently and effectively. The performance of reliability of the system was tested and it gained acceptance. The system was implemented successfully.

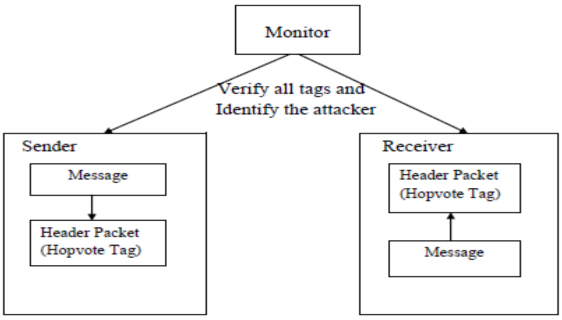


Fig-4: System Architecture Design

Proper implementation is essential to provide a reliable system to meet organization requirements. During the implementation stage a live demon was undertaken and made in front of end users. Implementation is a stage of where the system design is turned into a working system. This intends for testing the developed program with sample data, Detection and correction of internal error, testing the system to meet the user requirement, Feeding the real time data and retesting. Making necessary changes as described by the user.

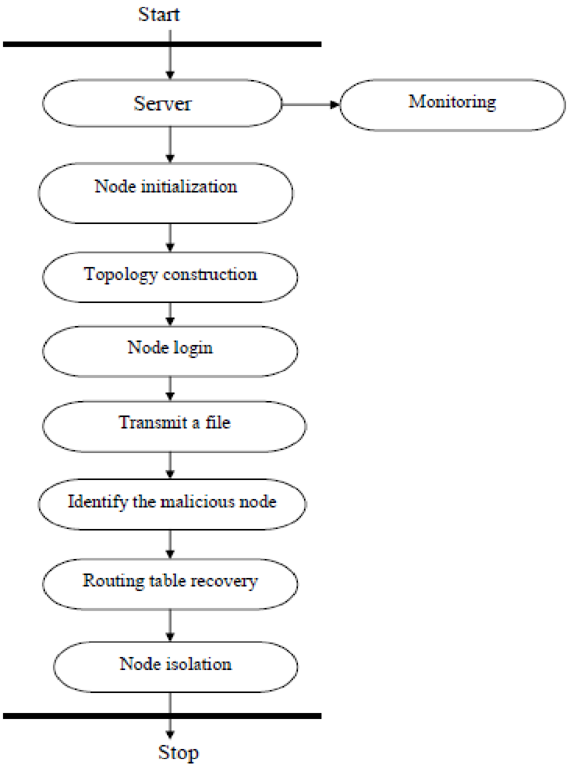
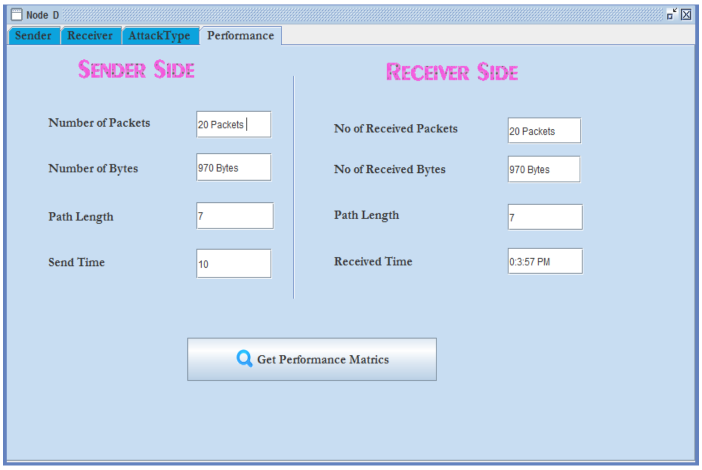


Fig-5: MARK mechanism



SENDER SIDE

Number of Packets: 20 Packets

Number of Bytes: 970 Bytes

Path Length: 7

Send Time: 10

RECEIVER SIDE

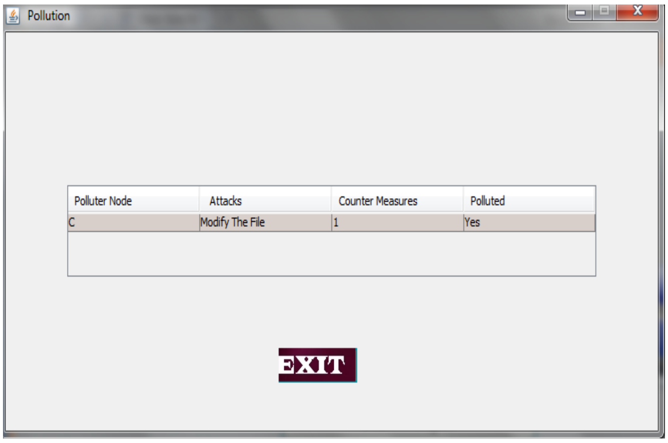
No of Received Packets: 20 Packets

No of Received Bytes: 970 Bytes

Path Length: 7

Received Time: 0:3:57 PM

Fig-6: Performance



Polluter Node	Attacks	Counter Measures	Polluted
C	Modify The File	1	Yes

Fig-7: Polluter Node

5. CONCLUSION

I have proposed a Mark based response solution for pollution attacks in the network. Especially, this approach considered the potential damages of data attacks and countermeasures to overcome the pollution activity. In order to measure the risk of both attacks and data recovery the MARK mechanism is used. This system extended the work of pinpointing the attacker node to the monitor with an attack type. Based on several metrics, this system is investigated the performance and other security approach and the experiment results clearly demonstrated the effectiveness and scalability of this proposed Mark mechanism approach.

6. FUTURE WORK

This study presents initial work in detecting misbehaving nodes and other pollution in the wireless networks. This section is described about some further ideas to explore in the future. The next goal is to analyze how the routing extensions perform with flows common to most network applications. The focus would then change from measuring throughput, or dropped packets, to measuring the time to complete a reliable transmission. Security is such an important feature that it could determine the success and wide deployment of wireless networks. A variety of pollution attacks have been identified. Security must be ensured in the entire system including the security primitives, such as key management protocols, since overall security level is determined by the system's weakest point.

ACKNOWLEDGMENTS

I take this opportunity to acknowledge with great Pleasure, deep satisfaction and gratitude, the contribution of many individuals in the successful completion of this project.

I express my profound sincerity and heartfelt gratefulness to chairman Thiru.V.S.Balsamy, B.Sc.,L.L.B., of V.S.B.College

of engineering, Karur, for having given me the opportunity to work and to undertake the project work.
I also express my gratitude to all the faculty members of Department for their timely support and encouragement. I thank my beloved parents and friends who have helped me to complete this project successfully.

REFERENCES

[1] Agrawal.S and Boneh.D (2009), "Homomorphic MACs: MAC-Based Integrity for Network Coding," Proc. Intel Conf. Applied Cryptography and Network Security.
[2] Dong.J, Curtmola.R, and Nita-Rotaru.C (2011), "Practical Defenses against Pollution Attacks in Wireless Network Coding," ACM Trans.Information and System Security, vol. 14, no. 1, article 7.
[3] Gennaro.R, Katz.J, Krawczyk.H, and Rabin.T (2010), "Secure Network Coding over the Integers," Proc. 13th Intel Conf. Practice and Theory in Public Key Cryptography (PKC "10).
[4] Ho.T, Medard.M, Koetter.R, Karger.D.R, Effros.M, Shi.J, andLeong.B, (2006) "A Random Linear Network Coding Approach to Multicast," IEEE Trans. Information Theory, vol. 52, no. 10, pp. 4413-4430.
[5] Jaggi.S, Langberg. M,Katti.S,Ho.T, Katabi.D, Medard.M and Effros.M(2009), "Resilient Network Coding in the Presence of Byzantine Adversaries," IEEE Trans. Information Theory, vol. 54, no. 6, pp. 2596-2603.
[6] Jiang.Y, Zhu.H, Shi.M, Shen.X, and Lin.C (2010), "An Efficient Dynamic- Identity Based Signature Scheme for Secure Network Coding," Computer Networks: The Intel J. Computer and Telecomm. Networking, vol. 54, no. 1, pp. 28-40.
[7] Krohn.M, Freedman's, and Mazieres.D, (2004)"On-the-Fly VerificationofRateless Erasure Codes for Efficient Content Distribution,"Proc. IEEE Symp. Security and Privacy.
[8] XiaohuWu, YinlongXu, ChauYeun and Liping Xiang (2014), "A Tag encoding scheme against pollution attack to linear network Coding" networking: transaction on parallel and distributed systems vol 25, no1.
[9] Yu.Z, Wei.Y, Ramkumar.B, and Guan.Y (2006), "An Efficient Signature- Based Scheme for Securing Network Coding against Pollution Attacks,"Proc. IEEE INFOCOM.
[10] Yun.A, Cheon.J, and Kim.Y (2010), "On Homomorphic Signatures for Network Coding," IEEE Trans. Computers, vol. 59, no. 9, pp. 1295-1296.
[11] Zhang.P, Jiang.Y, Lin.C, Yao.H, Wasef.A, and Shen.X.S (2011), "Padding for Orthogonality: Efficient Subspace Authentication for Network Coding," Proc. IEEE INFOCOM.

WEBSITES:

1. http://www.javatpoint.com
2. http://www.stackoverflow.com
3. http://www.codeproject.com
4. http://www.dzone.com
5. http://www.leetcode.com