ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Cryptography Based Misbehavior Detection For Opportunistic Networks

Dr. Gandi Satyanarayana[1]

G. Sai Sravani[2], D. Sai Seakhar[3], V. Sri Likita[4], B. Hari Priya[5]

1Professor, Dept. of CSE, NS Raju Institute of Technology Visakhapatnam, Andhra Pradesh, India
2, 3, 4, 5 Student, Dept of CSE, NS Raju Institute of Technology Visakhapatnam, Andhra Pradesh, India
Drgandisatyanarayana.cse@nsrit.edu.in, sravaniyadav903@gmail.com, sai.sekhar.1998@gmail.com, haripriyabobba@gmail.com, vslikita@gmail.com.

Abstract

Opportunistic networks (OppNets) are a subclass of Delay tolerant networks. To detect the misbehavior and trust control mechanisms in network nodes Opportunistic networks are proposed. They provide security in three different aspects: Trust, Privacy and Security. The trust-based mechanism is capable of providing security in terms of access control in the network. But the trust-based mechanisms do not solve the problem of isolating, avoiding and detecting the malicious content on the nodes. But with the provision of security services such as authentication, confidentiality and message integration by the means of cryptography. A trust based routing technology is provided for detecting malicious nodes and also providing security through the cryptography mechanisms.

The application of security overlay helps in thwarting the malicious behavior and also increases the performance of the nodes up to 35%. A security framework has been designed for high-end computing mobile devices. The distributive and disruptive nature of OppNets restricts the use of third party for key distribution purpose. The framework is designed to provide hop-to-hop mutual authentication and end-to-end message integrity.

Keywords: Privacy, Cryptograpgy, Authentication, Networks and Framework.

1. Introduction

DELAY tolerant networks (DTNs) have recently captured the attention of network researchers due to the growing importance of these networks in a challenging environment. DTNs have a unique constraint of intermittent connectivity, which restricts the application of traditional routing protocols in DTNs. Most of the designed routing protocols for opportunistic networks (OppNets) use the nodes mobility for exploiting the contact opportunity in the network. In initial advancement, an infrastructure-based message ferrying concept is used for routing in OppNets. Furthermore, the history-based contact prediction mechanisms are also used and in these routing mechanisms a prediction about opportunistic contacts with destination node acts as a decision parameter for exchanging messages between the encountered nodes. The OppNet devices are usually carried by humans and hence the researchers also explored the impact of human mobility on routing for designing forwarding mechanisms. The study through complex networks analysis (CNA) provides a useful insight on the impact of human mobility toward routing. The CNA-based routings are utility driven where messages are forwarded to the nodes with higher utility.

Cite this Article as: Dr.Gandi Satyanarayana, G.S Sravani, D.Sai Seakhar, V.Sri Likita, B.Hari Pr "Cryptography Based Misbehavior Detection I Opportunistic Networks"s", International Journal Magazine of Engineering, Technology, Management a Research (IJMETMR), ISSN 2348-4845, Volume 7 Issue 2020, Page 14-23.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The CNA-based routing uses the socially driven utility metrics such as, similarity, betweenness, contact frequency, and last encounter time to name a few. The social characteristics such as communities, similarity, and centrality positively support the routing mechanisms. But, social selfishness of a node impacts the routing in negative terms. Incentive mechanisms are designed for thwarting selfishness and increasing the participation ratio of the network nodes. Incentive-based routing mechanisms are also being designed using trust-based reputation systems. In most of the trust-based routing mechanisms selfish nodes are either incentivized using trust for increasing participation or avoided in message passing through isolation. In real scenario a node may be willing to participate or collaborate in the network. But, collaborative nodes may participate with having a malicious intent in the network. Hence, the trust-based routing for addressing selfishness may collapse under malicious nodes misbehavior scenario.

In OppNets the trust-based mechanism can only provide the social security in terms of access control in the network. The trust is used as a utility in accessing the exchange vector between encountered nodes. The commercial application of OppNets demands the facilitation of security features in routing mechanisms. The context- and content-based OppNet routing has different inherent security requirements. The context-based routing requires the revelation of context or identity of nodes for routing. Hence, the privacy of identity of nodes is much more important for context-based routing, whereas the content-based routing requires the protection of message on the forefront.

The hop-to-hop and end-to-end authentication is ensured using asymmetric cryptography RSA and symmetric cryptography Diffie–Hellman, respectively. The message integrity and confidentiality are also ensured once the key is exchanged between a source and a destination node in the network. The suspicious nodes are first figured out in the network and then the spy nodes keep vigil on these suspicious nodes and finally declaring it malicious or a normal node. The maliciousness of the node is further reflected in the network through depreciation of trust for the concerned node.

The main contribution is the robust design of the security overlay, which provides adaptable security depending on the requirement of the underlying routing mechanism and the backward linkage of malicious detection through trust depreciation. The designed mechanism also works over the trust-based incentive protocol for addressing selfishness in the network. Hence, the design is an outlay for adaptable security service to opportunistic networks. The usage of established symmetric and asymmetric key cryptography provides the authentication, message confidentiality, and integrity in the network.

2. System Analysis

2.1 Existing System

- Currently, the trust and reputation based mechanisms are used to authenticate a node's identity and avoid malicious nodes.
- The trust based mechanisms checks whether the trust value of a particular node is above a threshold.
- The trust based mechanism are capable of providing social security in terms of access control in the network.
- Incentive-based routing mechanism are also designed on trust based reputation system for thwarting selfishness and increase participation.

2.2 Proposed System

- A security overlay is designed over trust based routing mechanism.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- Spy nodes keep careful watch over the participative nodes in the network.
- The hop-to-hop authentication using asymmetric cryptography.
- End-to-end authentication using symmetric cryptography.
- Suspicious nodes figured out and are under the supervision of the spy nodes.
- Spy nodes then declare it as malicious or as a normal node.
- Maliciousness of the node is modified by declaring the trust value.

3. System Specification

3.1 System Requirements

3.1.1 Hardware Requirements

- Hard Disk : 40GB
- RAM : 1GB

3.1.2 Software Requirements

- Operating System : Linux
- Coding Language : NS2
- IDE : Ubuntu
- Database : MYSQL

3.1.3 Functional Requirements

Functional requirements describe what the system should do, i.e, the services provided for the users and for other systems.

Input

- The service provider should give at least 51 nodes or more than that.
- The end user can insert more number of nodes.
- The service provider try to insert attackers for acquiring the information from the users.
- The end user will detect those attackers by using the malicious node detection techniques.

Output

- The service provider gets an output as performance evaluation of each and every node as he/she taken.
- The data transmission from node to node is done with the help of "provider" nodes.
- The in-between attackers are detected by the time-delay concept and malicious node detection techniques used in this.
- Every node has some unique ID and Identity which varies from node to node.

3.1.4 Non-Functional Requirements

In non-functional requirements are the things that come under the following

- **Reusability**: As we developed the framework for the implementation of the nodes in the message integrity can be re-used for any one without having any restrictions in its usage. Hence it is re-usable.
- **Extensibility**: The further implementation can be extended at any level if the userwish to extend that in future because it depends on the input what we given.

4. Designing The Framework

The commercial usage of Opp Nets demands the strengthening of security for the network. In reference to the security aspect, Opp Nets should be accustomed with important security features. The advancement in processing capabilities and urban usage of these smart devices facilitate the use of cryptography along with the established trust-based model in Opp Nets. Most of the trust-based routing Opp Nets is supposed to cater the identification and isolation of socially misbehaved nodes in the network. The identification of socially misbehaved nodes in the trust-based protocol is largely based on the centrality metrics such as constant frequency, contact duration, similarity, between ness and reciprocity.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

4.1 Security Model

The security framework in this, is designed to detect the malicious entity such as black hole, worm hole, and masquerade nodes in the network. The security framework has been designed for high-end computing mobile devices in dense urban areas. In an urban environment, the cumulative contact duration of nodes are more in comparison to rural sparse OppNets. The distributive and disruptive nature of OppNets restricts the use of trusted third party for key distribution purpose. It includes hop-to-hop authentication is taken care of through the holding of the public keys of immediate neighbors. The design provides an infrastructure-based solution for key sharing through the use of Diffie-Hellman key exchange protocol. The framework is designed to provide hop-to-hop mutual authentication and end-to-end message integrity. It mainly focuses only on targeting the black hole, wormhole and masquerading aspects of malicious nodes in the network.

In realizing the security framework, the nodes in the network are divided four nodes. They are:

- **Normal nodes** – Nodes without any malicious intent in it.
- **Malicious nodes** – Nodes with malicious content in it.
- **Spy nodes** – Nodes are used for spying on the network.
- **Judge nodes** – Nodes having the capability to judge the malicious nodes and to revoke the malicious nodes and alert the normal nodes.

The infrastructure nodes i.e., spy and judge nodes are assumed to be uncompromised nodes in the network. The security framework has been inspired from the intelligence network. The aim of this design is to detect the normal nodes from malicious nodes in the network. The spy and judge nodes play a major role in protecting and providing security to the network. The analogy of the proposed security framework compared with the intelligence network of the country is well supported by the following facts; the network of spy nodes in the framework is analogous to the executive wing of intelligence in a country and the judge nodes are the representative judiciary of a country in this model.

The cryptographic algorithm is used to provide message integrity, authentication, and confidentiality in the network. The use of cryptography ensures the temper proof intelligence and the application of asymmetric cryptography at hop-to-hop level also ensures the mutual authentication and digital signature. The design of the security framework facilitates in exchange of symmetric keys between the source and destination nodes. The exchange of keys uses the established Diffie Hellman key exchange protocol.

5. Performance Analysis

5.1 Simulation Setup

The proposed security model shown in Fig. 1 works as an overlay over the base trust-based routing used in the network. The trust-based routing only provides the social security, whereas the designed mechanism provides the cryptographic security as well. The designed mechanism not only identifies and isolates the malicious nodes in the network; it also affects the trust of the malicious nodes through the application of TAF. The judge nodes verify and give their verdict against the malicious nodes. On delivery the verdict judge node also specifies the scale of trust breachment. The scale of trust breachment is directly responsible for ascertaining the TAF, which is as follows:

TAFi α (Scale of Trust breachment of node i)

TAFi = k (Scale of Trust breachment of node i).

The value of TAFi is used as a foreign element for calculating the actual trust of the node.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

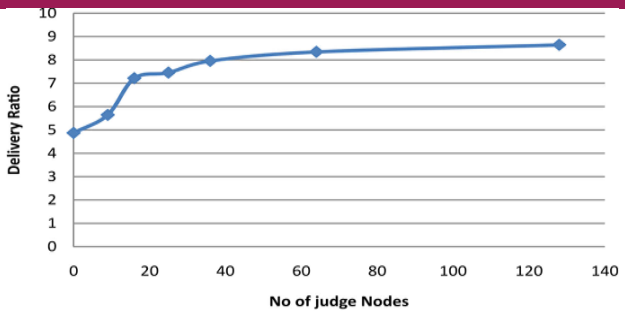

Fig 1: Delivery Ratio Versus Number of Nodes

The parameter associated with infrastructure nodes are depicted. The malicious and normal nodes are uniformly distributed throughout the network. The infrastructure nodes are fixed and placed in their respective assigned zone for detecting the malicious node. The malicious node has higher transmission power and range in comparison to normal nodes.

- we simulate performance of the proposed security overlay design

using SimBet as the base routing protocol. The spy and judge nodes are capable of detecting malicious behavior through the use of their respective defined pathway mobility model and procedures are defined below.

- The simulation compares the routing protocol is based on the

performance metrics: throughput, average end-to-end delay, malicious detection rate, false positive rate, MIM detection rate, and overhead cost. The design and use of a security protocol is constrained with some overheads. The count of overheads indirectly helps in estimating the cost incurred in the detection of malicious nodes. In order to keep the calculation simple, overheads involves the infrastructure cost of spy and judge nodes and the time loss incurred during the identification of the malicious nodes.

- The simulation compares the Simbet routing protocol is based on the

performance metrics: throughput, average end-to-end delay, malicious detection rate, false positive rate, MIM detection rate, and overhead cost. The design and use of a security protocol is constrained with some overheads.

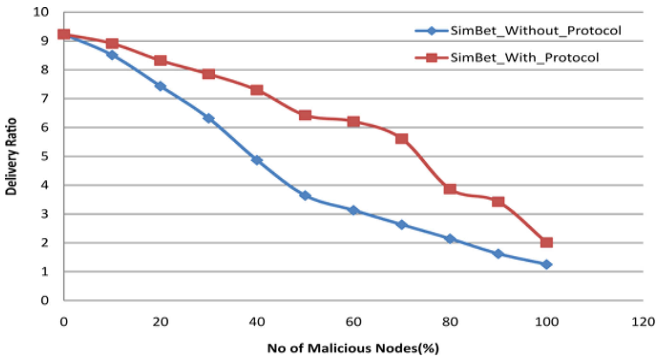

Fig 2: Delivery Ratio Versus Number of Malicious Nodes

The count of overheads indirectly helps in estimating the cost incurred in the detection of malicious nodes. In order to keep the calculation simple, overheads involves the infrastructure cost of spy and judge nodes and the time loss in curred during the identification of the malicious nodes. The graph in Fig. 2 depicts the throughput of SimBet with and without the application of designed security protocol. In normal situation, the delivery ratio of SimBet consistently drops with the introduction of more malicious nodes in the system.

As the behavior of malicious nodes involves, packet replay and black hole attacks. So, either the bandwidth is exhausted through replaying and leads to denial-of-service attack or black hole nodes acts as a sink for the encountered messages. So, the accumulative impact of these malicious nesses results in the degradation of throughout performance of SimBet. The delivery ratio drops from 9.2 to 1.2 with the introduction of 0 to 100 percent malicious nodes respectively.

6. Result Analysis

In normal situation, the delivery ratio of SimBet consistently drops with the introduction of more malicious nodes in the system. As the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

behavior of malicious nodes involves, packet replay and black hole attacks. So, either the bandwidth is exhausted through replaying and leads to denial-of-service attack or black hole nodes acts as a sink for the encountered messages. So, the accumulative impact of these malicious nesses results in the degradation of throughout performance of SimBet.

The delivery ratio drops from **9.2** to **1.2** with the introduction of **0** to **100%** malicious nodes, respectively. It also shows the impact of designed security protocol on delivery ratio and the application of security protocol on SimBet protocol helps in improving the delivery ratio on each percentage of maliciousness nodes count.

The designed protocol seems to be much more effective in the range of **40%** to **60%** of the malicious nodes. Here, the security protocol has almost improved the delivery ratio by **40%** from **3.12** to **6.21** at **60%** malicious nodes count.

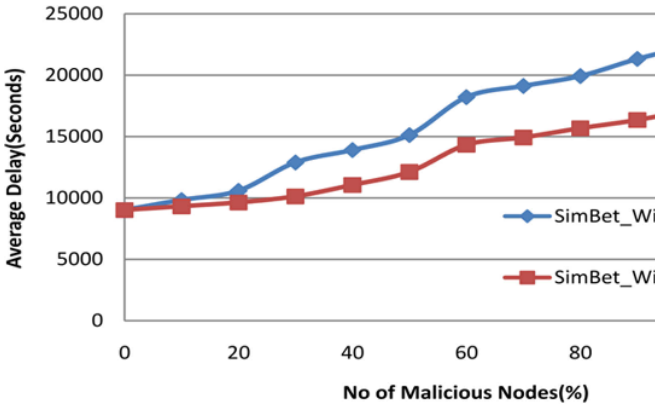

Fig 3: Average Delay Verus Number Of Malicious Nodes

The best delivery ratio of SimBet protocol is around **90%.** In the analysis we have seen drop in delivery ratio from **9.2** to **1.2**. In Fig. 6 analysis, the application of security overlay at best improves the delivery ratio from **3.12** to **6.21** with fixed **16** judge nodes. But the best possible delivery ratio is **9.2**. So we would analyze the impact of infrastructure count on the delivery ratio.

- The application of more number of judge and associated spy node's makes the malicious node's detection much more fast and precise. Hence with the increase in the judge nodes keeping the malicious nodes fixed at 40% helps in improving and achieving the delivery ratio.

- As the malicious nodes may also act as wormhole nodes in the network, which may decrease the average delay in the message transmission. So here in this simulation, malicious nodes are selectively avoided to form a wormhole regarding average delay analysis.

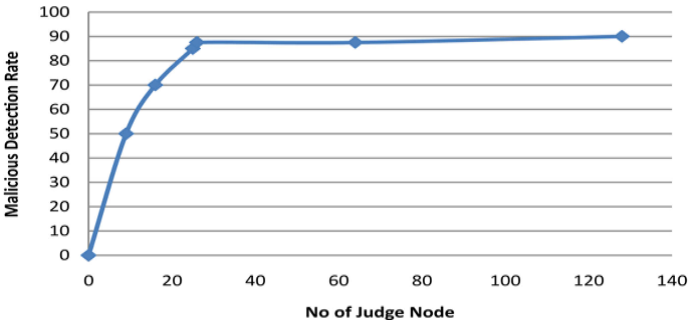

Fig 4: Malicious Detection Rate Versus Number of Judge Nodes

- The detection rate is **80%** at the malicious count of **10%.** But the detection rate reduces to just **45%** at the malicious count of **100%.** The average malicious detection rate of the security overlay is **60%** in the network for SimBet protocol.

- Here, in Fig. 5, the detection rate keeps on increasing for same as 40% malicious count with the increase in infrastructure nodes. The detection rate is almost 85% with 36 judge nodes and approaches to 90% with 128 judge nodes in the network.

- The increase in the judge nodes directly results in more number of spy nodes. The spy team are also associated with smaller spy zones in the network and hence there things able the infrastructure nodes to trace the malicious nodes effectively in less time.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

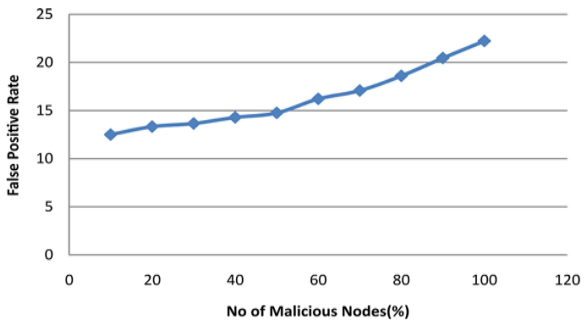

Fig 5: False Positive Rate Versus Number of Malicious Nodes

In fig 5 depicts the percentage of false malicious node's detection out of the complete detection in the network. The average false detection rate is 15% and this is considerably less for a protocol to be judged as reliable. The false detection rate varies from 12% to 22% for 10% to 100% malicious nodes in the network, respectively. Even the false positive rate can be minimized with the increase of infrastructure nodes in the network.

- The performance of the network increases as we increase the judge nodes in the network, with **16** judge nodes and **40%** of the malicious nodes, the detection rate is **70%.** As the number of judge nodes increases in the network, the detection rate also increases with almost **85%** detection rate with **64** judge nodes.

- The application of 36 nodes helps in achieving **90%** detection rate but here in Fig 8.2 even after the application of **64** judge nodes only helps in achieving **85%** detection rates. The MIM attacks in distributed, sparse, and delay-tolerant characteristics make the tracing of MIM nodes in the network highly difficult.

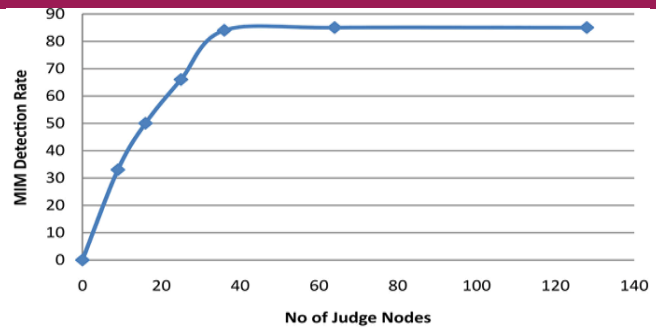

Fig 6: Mim Detection Rate Versus Number of Judge Nodes

Fig 7 shows analysis of the detection rate of MIM attacks in the network. The detection rates are analyzed for the situation where out of 40% of the malicious nodes 15% of the nodes are attributed with MIM attacks. The MIM detection rate is 33% with 9 judge nodes.

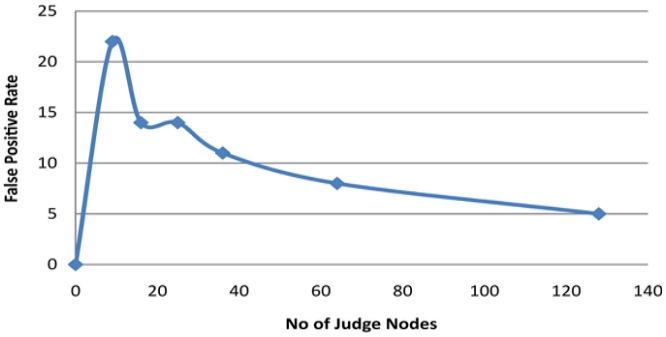

Fig 7: False Positive Rate Versus Number of Judge Nodes

In Fig. 7, the false positive rate decreases from **22%** to **5%** with the increase of judge nodes from 9 to 128 in the network at **40%** malicious node count. The increase of judge nodes indirectly helps the spy teams to work and snoops over the smaller region. Hence, the spy teams effectively figured out and label malicious nodes precisely in the network.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

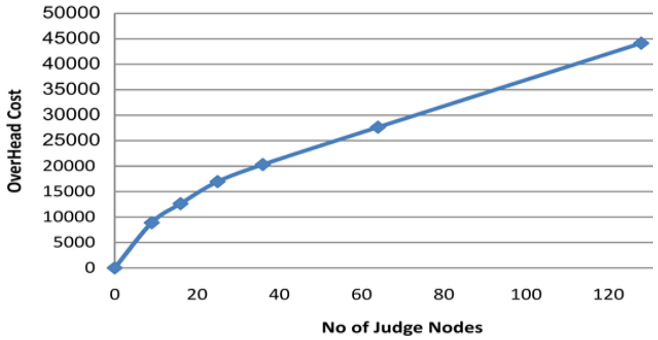

Fig 8: Overhead Cost Versus Number of Judge Nodes

Hence, the tracking of MIM nodes requires more infrastructure than compared to other malicious activity in DTNs. The overhead associated with the application of security overlay is depicted. The overhead includes the infrastructure cost and the time lag associated in identification of malicious nodes in the network.

- The minimum delay of the SimBet protocol without malicious nodes is around 9000's.But with the introduction of malicious nodes the average delay increases in each step. The application of security protocol helps to figure out the malicious nodes and avoid them through trust depreciation. The tradeoff between performance and cost restricts the security design to use unlimited number of infrastructure nodes in the network.

6. Conclusion

The proposed framework has established that the amalgamation of cryptographic features and infrastructure surveillance helps in providing are liable security service and detecting the malicious nodes in the network. The simulation results have further strengthened and proved that the application of security overlay helps in thwarting the malicious behavior and increasing the average performance by **35%.** The performance of this work depends upon the number of infrastructure nodes. Hence, there is a tradeoff between security performance and energy usage in the system. In future, we would like to address the energy efficiency issue and intent to reduce the cost associated with malicious detection through the use of infrastructure nodes and robust-dynamic mobility model of the surveillance nodes in the network.

Opportunistic networks (OppNets) are a subclass of Delay tolerant networks which are used to detect the misbehavior and trust control mechanisms in network nodes Opportunistic networks are proposed. They provide security in three different aspects: Trust, Privacy and Security. The trust-based mechanism is capable of providing security in terms of access control in the network. A trust-based routing technology is provided for detecting malicious nodes and also providing security through the cryptography mechanisms.

7. Output Screens

The following figures are the output for the data transmission from source node to destination node. Each node has some unique ID & IDENTITY.

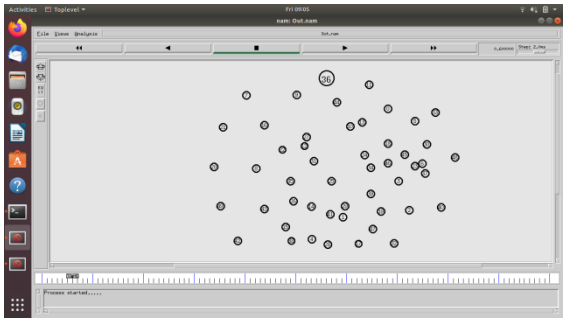

Fig 9: Node Specification

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

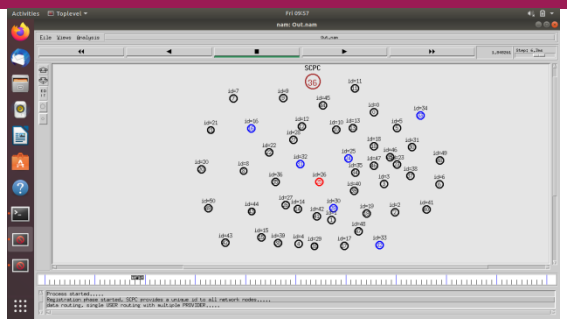

Fig 10: Each Node with Some Unique Id

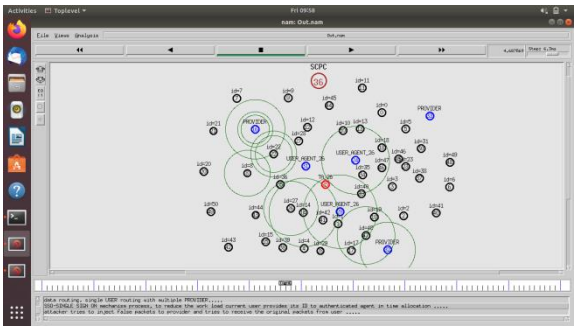

Fig 11: Data Transmission from Source to Destination Nodes

The above fig tells that the data transmission from source node to destination node through providers in between them.

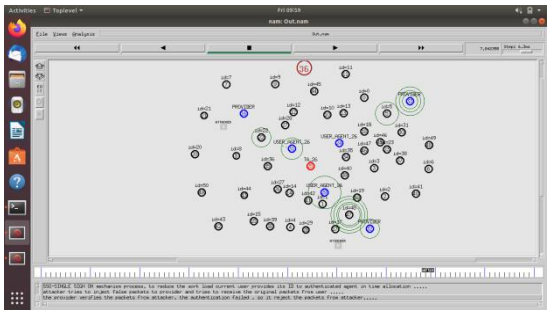

Fig 12: Arrival of Attacker Nodes

The fig-12 shows the arrival of attacker nodes. Whenever the attacker nodes enter into the network to acquire the data from the nodes while transferring the data from source to destination through the provider's. Therefore, there is a chance to loss the data while transferring it. To detect these malicious nodes we are using hashing techniques.

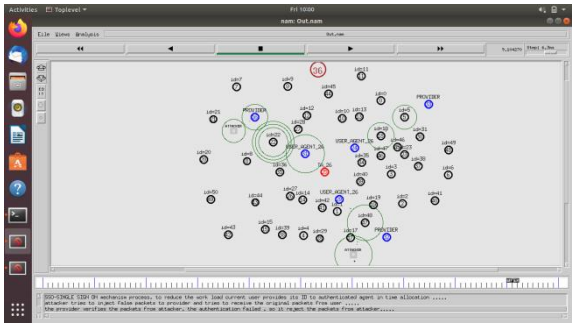

Fig 13: Detection of Attacker Nodes

The fig shows the detection of attacker nodes by using the Hashing Function. Here the user helps to provides the ID to authentication agent for each node by using the Trust Authority (TA).

8. References

1) https://searchsecurity.techtarget.com/definition/cryptography
2) https://doubleoctopus.com/security-wiki/encryption-and-cryptography/diffie-hellman-algorithm/
3) https://www.igi-global.com/dictionary/delay-tolerant-networks/21334
4) https://en.wikipedia.org/wiki/Delay-tolerant_networking
5) https://en.wikipedia.org/wiki/Opportunistic_mobile_social_network
6) K. Fall, "A delay-tolerant network architecture for challenged internets," In Proc. 2003 Conf. Appl., Technol., Archit., Protocols Comput. Commun., New York, NY, USA, pp. 27–34, 2003, doi: 10.1145/863955.863960.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

7) Y. Zhu, B. Xu, X. Shi, and Y. Wang, "A survey of social-based routing in delay tolerant networks: Positive and negative social effects," IEEE Commun. Surveys Tuts, vol. 15, no. 1, pp. 387–401, Jan–Mar. 2013, doi:10.1109/SURV.2012.032612.00004.

8) K. Wei, X. Liang, and K. Xu, "A survey of social-aware routing protocols in delay tolerant networks: Applications, taxonomy and designrelated issues," IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 556–578, Jan–Mar. 2014 , doi: 10.1109/SURV.2013.042313.00103.

9) M. E. Newman, "The structure and function of complex networks," SIAM Rev., vol. 45, no. 2, pp. 167–256, 2003.

10) N. Magaia, A. P. Francisco, P. Pereira, and M. Correia, "Betweenness centrality in delay tolerant networks:Asurvey," Ad Hoc Networks, vol. 33, pp. 284–305, 2015, doi: 10.1016/j.adhoc.2015.05.002.

11) X. Jiang and X. Y. Bai, "A survey on incentive mechanism of delay tolerant networks," in Proc. 10th Int. Comput. Conf.Wavelet Active Media Technol. Inf. Process., Chengdu, China, 2013, pp. 191–197, doi: 10.1109/ICCWAMTIP.2013.6716629.

12) W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," ACM Comput. Surveys, vol. 45, no. 4, Aug. 2013, Art. no. 47, doi: 10.1145/2501654.2501661. R. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21 no. 2, pp. 120–126, Feb. 1978.

13) W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654, Nov. 1976, doi: 10.1109/TIT.1976.1055638.

14) L. Wei, H. Zhu, Z. Cao, and X. Shen, "SUCCESS: A secure user-centric and social-aware reputation based incentive scheme for DTNs," Ad Hoc Wireless Sensor Netw., vol. 19, no. 1/2, pp. 95–118, 2013.

15) G. Bigwood and T. Henderson, "Ironman: Using social networks to add incentives and reputation to opportunistic networks," in Proc. IEEE 3rd Int. Conf. Privacy, Security, Risk Trust 2011 IEEE 3rd Int. Conf. Soc. Comput., 2011, pp. 65–72.