International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7209
***Article Received**: 27 April 2023 **Revised:** 15 June 2023 **Accepted:** 29 June 2023*

Secured Scheme for Privacy Preserving and Node Authentication Mechanism for a Special Mobile Ad hoc Network

Sushil Kumar Mishra, Ruchika Gupta
Department of Computer Science & Engineering, Chandigarh University, India
Corresponding Author: sushiljune@gmail.com

Abstract: Opportunistic networks are a special type of Mobile Ad hoc network which are wirelessly interlinked nodes with the absence of end to end connectivity. All nodes in an opportunistic network are free to move in an environment. Due to the high degree of mobility of nodes, opportunistic networks differ significantly from the existing traditional networks and it works on store, carry &forward mechanism in which, each node has a communication range. Within its proximity, if any node comes, it can send and receive messages. In an opportunistic network, there is no proper infrastructure available for communication and node have limited storage and computational capabilities. The major problem being faced in an opportunistic network is the identification of normal and malicious nodes because due to the open nature of the opportunistic network, malicious nodes also can join the network and perform some malicious activities like Sybil attack. We propose a remedy to address the authentication and privacy issue that can arise in an opportunistic network. According to the findings of the simulation, the proposed research work satisfies the authentication and privacy criteria of an opportunistic network.

Keywords: Opportunistic Network, Traditional network, Authentication, Privacy etc.

I. INTRODUCTION

Opportunistic network is used to create a reliable network which consists of multiple mobile nodes having limited storage, computational capacity with limited battery backup. These attributes led to researchers to focus on security, authentication, and privacy challenges in opportunistic networks [1]. In the absence of end-to-end connectivity, opportunistic networks have been evolved from delay tolerant networks. A number of wireless nodes connect to one another in an opportunistic network using a store, carry, and forward transmission mechanism. Due to mobile nodes in an opportunistic network, a frequent connection breakdown and delay in communication is a normal routine [2]. The architecture of an opportunistic network confronts significant challenges, such as determining how to successfully authenticate a node and ensuring routing security. Opportunistic networks, as opposed to delay-tolerant networks, require an opportunistic routing technique [3][4]. Finding the end-to-end path between the source and destination nodes is the first step when a message needs to be transmitted over a delay tolerant network. However, in opportunistic networks, messages are always transmitted opportunistically, based on a store, carry and forward mechanism [5]. Disaster management, wild life monitoring and battle field communication is a kind of application of opportunistic network [6]. In this article, we present a trust based algorithm to calculate trust value of each node which is part of an opportunistic network in an opportunistic network. A centralized node is known as a Leader node. It is responsible for registration of new node in an opportunistic network. But this creates a fixed structure framework for registration of new node. In the proposed mechanism, we have presented a decentralized mechanism for node registration in which a leader node selects a new node having a trust value more than minimum threshold value is known as Co-Leader which is also responsible for node registration. The authenticated nodes also compute the trust value of encountered nodes and share it with Leader node. Any authenticated node having higher trust value is being authorized for node registration by leader node is known as Co-Leader node. Figure-1 shows a store, carry, and forward mechanism where each node has communication range, computing capacity and storage. If two nodes are within its transmission range, they share messages with each other. If a message retransmission criteria are met. Finally, a message is propagated through a chain of intermediate nodes by opportunistic contact with the destination node.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7209
***Article Received**: 27 April 2023 **Revised:** 15 June 2023 **Accepted:** 29 June 2023*

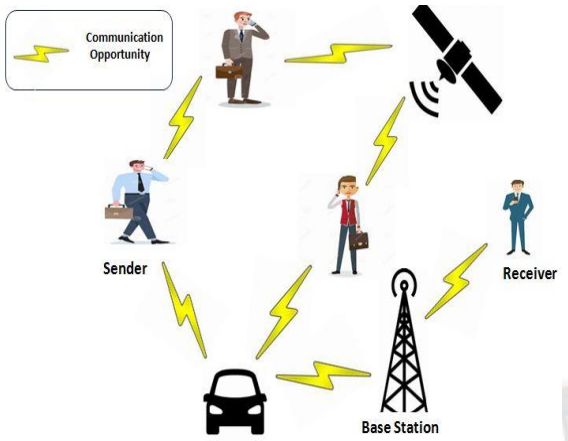

Figure-1: Communication in an opportunistic network

II. SECURITY CHALLENGES IN AN OPPORTUNISTIC NETWORK

Security threats are one of the main problems for opportunistic networks due to lack of end-to-end connectivity. Figure-2 represents the different types of security threats in an opportunity network.

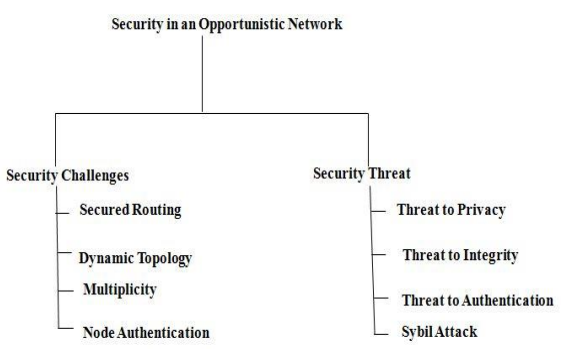

Figure-2: Security threat & Challenges

2.1 Security challenges in an Opportunistic Network

a. Secured Routing: Routing mechanisms is one of the security challenges in an Opportunistic network, due to its mobility nature of node, a node join or leave the network any time. In opportunistic networks, the store, carry & forward routing strategy increases packet delivery rate but come with significant delays and security problems. From a security perspective, the intermediary node (the malicious node) has the potential to compromise reliability, integrity, and privacy.

b. Dynamic Topology: In an opportunistic network, each node having storage and computational capabilities, but or devices are mobile node. They keep changing its location and direction with time, hence topology of opportunistic network is not fixed, its dynamic.

c. Multiplicity: Due to the lack of full network connectivity, opportunistic networks suffer. These networks may use a range of various forms of communication across multiple heterogeneous networks, which inevitably leads to identify and routing issues. Since node addresses across networks are not all the same, new procedures for trust and authentication must be implemented. d. Node authentication: In an opportunistic network, it is very difficult task to register only legitimate or authenticated nodes while avoiding malicious nodes from joining the network.

2.2 Security threat in an opportunistic network

a. Threat to Privacy: In an opportunistic network, each node is free to join or leave the opportunistic network due to mobile nodes. It provides an equal opportunity to all legitimate and malicious nodes to join the network [7]. If a malicious node is a part of network, it may publically disclose the information. It is direct a threat to privacy.

b. Threat to Integrity: An opportunistic network provides an open platform to all available nodes to be part of network. A compromised node easily can manipulate the information within network and circulate compromised information to all authenticated nodes. It leads to thread to integrity.

c. Threat to Authentication: Due to open nature of opportunistic network, all nodes can join the network. To deal with authentication issue, we need to implement an authentication mechanism to allow only legitimate node to join the network.

d. Sybil Attack: Sybil attack is used to create a several identity address and try to take control over network. The main aim of this type of attack is to take control over network and execute some malicious code to compromise the communication medium.

III. LITERATURE REVIEW

As previously discussed, due to node mobility and frequent node disconnection, authentication and security is one of the most complex issues in an opportunistic network, in the literature review process, all the existing literatures regarding authentication and security are reviewed to find out the exact protocols, shortcomings for future work. S. Rashidibajgan et al. 2022 proposed a mechanism to improve the performance of real time application with the help of machine learning technique [8]. S. Rashidibajgan et al. 2021 proposed a secured framework in order to select an appropriate adjacent node to convey the message towards destination [9]. The proposed technique forwards messages to intermediate

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7209
***Article Received**: 27 April 2023 **Revised:** 15 June 2023 **Accepted:** 29 June 2023*

nodes without taking prior node histories into account. The proposed technique also protects source node, intermediate nodes, and destination node identities and locations. Rashidibajgan et al. 2019 marked a new privacy preservation routing algorithm for the purpose of message transmission, a history table is created for each node participating in an opportunistic network, and past tracking data is recorded but kept secret from other nodes. In this routing strategy, an optimized routing decision is made based on the network nodes' prior interactions 10]. Y. Mao et al. 2019 proposed a secured probabilistic routing scheme based on past based encounters [11]. In the proposed protocol, we calculate the predictability of delivery according to encounter frequency between nodes. Two scheduling mechanisms are proposed to extend the traditional PROPHET protocol and improve both storage and transmission performance over the DTN. E. K. Wang et al. 2018 presented an effective model for an opportunistic network in which the decision is made based on a node's behavior, and input of other nodes [12]. Li, F. et al. 2017 proposed a social energy-based routing protocol in which decision for route selection is done based low power consumption [13]. Chen, K et al. 2017 presented a mechanism, used to imply real ids across all adjacent nodes in the act of an encounter, and communicates silently to preserve anonymity [14]. When these nodes separate from one another, all involved nodes are provided the encountered evidence in order to enable the actual utility. Guo, M et al. 2015 presented a security framework for privacy protection and authentication in an opportunistic network 15]. In this technique, Leader nodes control the authentication process and are in charge of node registration, ensuring that only valid nodes can join an opportunistic network. Additionally, this plan offers security mechanisms against various security threats and assaults. C. Xi, S. Liang et al. 2015 presented a scheme for behavioral input from nodes in an opportunistic network; a trust management approach has been developed [16]. Nodes are notified positively when a packet gets transmitted and negatively when a packet is dropped. Goyal et al. 2013 proposed privacy framework for opportunistic network where data is sent from the source to the destination node [17]. Super node is a special node that carries information of all the legitimate nodes and gives a virtual ID to all the legitimate nodes. This privacy framework can be used to address the security issue in the opportunistic network. B. Poonguzharselvi1 et al. 2012 proposed a safe way to forward data in an opportunity network [18]. Nodes that are voluntarily and temporarily connected form an opportunity network. Since there are no end-to-end connections, performing and implementing routing protocols to find and forward the message is very difficult. Nodes in this kind of network act according to mobility model. The next node to forward the data is selected based on the trust value and the direction of the nodes towards the destination nodes. Jian Ren et al. 2010 proposed a scheme MAAS (Message Anonymity Assurance) which is a message-based authentication scheme that incomes a targeted node, enables data transfer from the source node, and prevents malicious nodes from inferring a target node. MAAS improves transmission security while preserving the target node [19]. Greede et al. 2009 suggested a repository-based transfer protocol [20]. Each node maintains a vector table, and each vector table contains a node class, node address, and transmission range. When two nodes are within range, they share table's vector and start exchanging messages.

IV. PROPOSED METHODOLOGY

In this study, we provide a way of authenticating a node that have not yet authenticated in an opportunistic network and are not connected to a Leader node. In previous work, the registration and authentication mechanism required each new node to register at a static node. Here, the Leader node is one that has a high trust value. Such nodes are easily verified and have a high level of trust. We utilize two variables to determine the trust value. First counter is to track successfully delivered message to the end node and second messages delivered to middle nodes. Each node stores trust value for other nodes in a trust vector. Authority is awarded to the node exhibiting a highest trust value for registration by Leader node is known as "Co-Leader Node" when, they contact each other.

a. Leader Node: Leader is a node in an opportunistic network with highest trust value. It is responsible for registration and authentication of unauthenticated nodes and provides credential for authentication to be communicated with other authenticated nodes.

b. Co-Leader Node: These nodes are authenticated nodes and authorization is provided by Leader node for registration and authentication based on higher trust value as compared to threshold trust value.

4.1 Presumption for Node

The following assumptions are taken for mobile node in an opportunistic network:

a. Mobile phone, tablets are assumed here as a node. Each mobile node has computational and storage capacities.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7209
***Article Received**: 27 April 2023 **Revised:** 15 June 2023 **Accepted:** 29 June 2023*

b. New mobile node in an opportunistic network must register at a leader or Co-Leader node only.

c. Leader or Co-leader nodes are responsible for registration and authentication.

d. All mobile nodes in an opportunistic network communicate with each other wirelessly.

Table 1: Symbol Table

Symbol	Description
N_X	*Node X (New Node for process initiation)*
N_L	*Leader Node*
N_C	*Co-Leader node*
MSG	*Message*
IN	*Identity number*
TS_i	*Time Stamp of i^{th}Node*
TS	*Threshold Time Stamp*
NC	*Number of NC*
TTV	*Threshold Trust Value*
DCT	*Docket*
PUK_i	*Public key for i^{th}node*
PRK_i	*Private key for i^{th}node*
CPT	*Ciphertext*
PLT	*Plaintext*
$MSG_{X,Y}$	*Number of message successfully transferredfrom N_X to intermediate node N_Y*
$MSG_{X,L}$	*Number of message successfully transferred from $N_X$to destination N_L*
MSG^*	*Data forwarded to any node in an Opportunistic network*
DF( )	*Data forward*
$CV_{X,Y}$	*Number of time transmission successfully ofN_X at N_Y*
$TV_{X,Y}$	*Trust value of $N_X$at N_Y*
W	*Number of times $N_X$encounters a node*
TV_X	*Aggregated trust value of N_X(x…n)*

T Table 1 is representing symbols and descriptions of used variable.

4. 4.2 Registration and Authentication Phase

When, new node enters in an opportunistic network environment. It is mandatory to all new mobile nodes to register and authenticate itself at Leader (N_L) or Co-Leader node(N_C).The procedures for authentication and registration are described below.

I In registration phase, new node can request for registration with both nodes Leader node (NL) and Co-Leader nodes (N_C) but one at a time.

Step1 : New mobile nodes N_X forward a request $h(MSG)||h(IN_{Nx})$ with TS_{NX} for registration at Leader node (N_L) or Co-Leader nodes (N_C).

Step2 : Leader node (N_L) or Co-Leader nodes (N_C) responds to a request forwarded by new node NX after checking the validity of TS_{NX}<= TS, if it is valid then forwards the response

$h(MSG)||\ h(IN_{Nx})$ XOR PUK_{NL} with $TS_{NL.}$

Step3: Node (N_X) receives response from N_L or N_C and check the validity of TS_{NL}<= TS. If it is valid then forward acknowledgement to N_L or N_C.

Step4: N_L or N_C with help of Elgamal algorithm, produce private and public key with TS_{NL} for node NX.

D Docket DCT= $(h(MSG)||\ h(IN_{Nx}), PRK_{NX})$ XOR (PUK_{NX})

DCT is encrypted by public key. Where, DCT keeps identification number of node N_x, PRK_{NX} and PUK_{NX} and it is forwarded to N_X with TS_{NL}.

St **Step5:** N_X receiving response from N_L or N_C, check the validity TS_{NL}<=TS. If it is valid then extract.

: **Step6:** N_X sends acknowledgement to N_L or N_C for the same with $TS_{NX.}$

Step7: Upon receiving acknowledgement, N_L or N_C checks the validity of TS_{NX}<=TS. If is valid then initiate process to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7209
***Article Received**: 27 April 2023 **Revised:** 15 June 2023 **Accepted:** 29 June 2023*

add node N_X in authenticated node list and update the public key list for all authenticated nodes. Figure-3 is showing a mechanism for node registration and authentication.

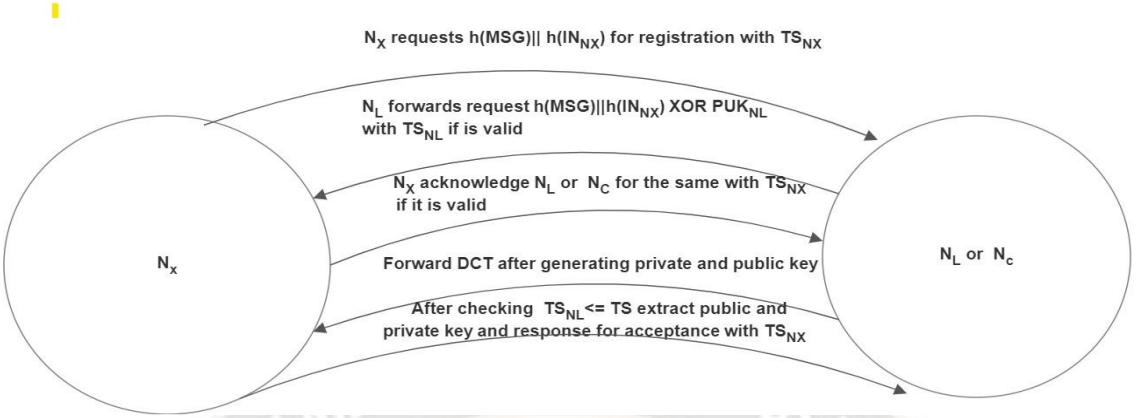

Figure-3: Registration and Authentication Phase

4.3 Message Encryption

In the encryption mechanism, whenever node N_X forwards a message to Node N_Y. Node N_X uses public key of Node N_Y.

Primary Ciphertext $CPT1=EK1^{RN}MOD(A)$

Secondary Ciphertext $CPT2=(PLT*EK2^{RN})\ MOD(A)$

Complete Ciphertext $CPT=(CPT1, CPT2)$

4.4 Message Decryption

In decryption process, node N_Y accepts ciphertext (CPT) from Node N_X and decrypt it by using its own private key (PRK_{NX}).

$PLT = [CPT2*(CPT1PRK)-1]MOD(A)$

4.5 Authentication

Due to the suggested authentication approach, all nodes must verify public list of Leader node before transmitting or accepting any messages If public key of node is not present in public key list of a Leader node. That means node is not authenticated. By using this approach, node authentication is achieved.

4.6 Privacy

Leader node and Co-Leader nodes process all request in cipher text format at the time of proposed authentication mechanism. No textual information was saved which regularly protect data privacy. In an opportunistic network, all nodes keep moving in network environment and no topology is maintained which helps to maintain location privacy.

4.7 Scheme for Trust Computation

In this scheme, if any node is part of an opportunistic network. Its trust value is calculated and it is stored in trust vector. Trust calculation is done based on two factors: successfultransferred of message from source node to intermediate node (NY) and end node (NL) andnumber of contacts in an opportunistic network.

Algorithm1:Trust Calculation for Each Node in Network (TCN)

Input: First initialize all parameters

$MSG_{X,Y}$: 0 , $MSG_{X,L}$: 0

$TV_{X,Y}$: 0 , $TV_{X,L}$: 0

$CV_{X,Y}$: 0

Output: Trust Computation of all nodes

While(N_X is not (N_L|| N_C))

{

If(N_X has successfully transmitted data and received acknowledgement to N_Y) then

$MSG_{X,Y}= MSG_{X,Y}+1$

If (N_X encounters N_Y (Intermediate node)) then

$CV_{X,Y}=CV_{X,Y}+1$

Calculation of trust value ($TV_{X,Y}$)= ($MSG_{X,Y}$)/ ($CV_{X,Y}$)

If(N_X encounters N_L) Then

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7209
***Article Received**: 27 April 2023 **Revised:** 15 June 2023 **Accepted:** 29 June 2023*

Trust value of N_X at N_L=TV_X/W }

4.8 Scheme for Co-Leader Node (N_C) by Leader Node (N_L)

In an opportunistic network, leader node is responsible for registration and authentication of a new joining node. It is a static strategy for registering and authenticating a node. In the new strategy leader node N_L provides rights to some other node having trust value more than a threshold trust value is known as Co-Leader. If any Co-Leader having trust value less than threshold value, then its authorization leads to cancellation.

Algorithm2: Authorization by Leader node to Co-Leader node(ALC)

Input : Initialize all parameter

TTV >=1

NC: 0 (At initially stage)

$TV_{X,L}$: 0

Output : Authorization for NC

If($TV_{X,L}$ is greater than TTV)

then

/*NL updates trust value in its trust vector and authorize it for registering and authenticating new node*/

NC=NC+1

Else if (N_X=N_C && $TV_{X,L}$ is less than TTV)

/*N_L removes authorization of NC node and update in its record */

NC=NC-1

4.9 Data Routing Mechanism

In this routing, mechanism is prepared for forwarding data in an opportunistic network based on trust value in Trust Vector. In this mechanism, trust value of each node is compared with each other, and data is forwarded with a node having higher trust value in Trust Vector.

Algorithm3:Data advancement in an opportunistic network

If (DF((MSG, NY)==1||((MSG, N_L)==1))

then

$MSG^*=MSG^*+1$

Else If(MSG Is not forwarded)

/ MSG is not forwarded due to any reason */ then*

$MSG^*= MSG^*$

/ MSG^*remains same. it affects the trust value * /*

Algorithm4:Procedure for route selection

For DF(N_X, N)

/ N is representing all node in an opportunistic network */*

Data is sent to any node N in an opportunistic network with higher trust value(T1---N)

DF(MSG,N)

/ where N is a node with higher trust value among all available node in proximity */*

V. SIMULATION WORK AND EXPERIMENTAL SETUP

The proposed routing algorithms is implemented on an open source '*One Simulator*' to compute performance metric as compared to existing spray and wait routing algorithm. Table 2 represents simulation parameters used.

Table 2: Simulation Parameters

Parameter	Value
Simulation Area	1000 m*500m
Communication Range	250 m
Communication Rate	3mbps
Message Size	500KB
Number of Nodes	50-110

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7209
***Article Received**: 27 April 2023 **Revised:** 15 June 2023 **Accepted:** 29 June 2023*

Performance Metrics: The following performance metrics are considered in order to implement the proposed algorithm:-

Delivery Ratio: Delivery ratio is referred as a proportion between total message delivered (TMD) and message created (TMC). It is represented by DRi.

$$DRi = TMD/TMC$$

Network Latency: Network latency refers to the time delay experienced in data transmission over a network. It represents the time taken for a data packet to travel from the source to the destination across the network. It is represented by NLi.

Where message delivered in network and message generated in network are represented by MDN and MGN

N Li = [(MDN) – (MGN)]

VI. EXPERIMENTAL RESULT

The proposed mechanism is simulated on "One simulator" and contrasted with the present *spray & focus* approach to determine the delivery ratio and network latency. According to Figure-4, the delivery ratio in an opportunistic network is directly proportional to the number of nodes. This is simply because our proposed authentication mechanism examines malicious nodes and restricts them from joining the network. This mechanism ensures fewer messages dropping which results higher delivery ratio. The suggested approach outperformed the spray & focus algorithm in terms of performance.

Figure-5 is representing network latency for our proposed algorithm against spray and focus algorithm and shows better network latency ratio as compared to spray and focus algorithm. For implementation of our proposed algorithm, no data is shared in plaintext form. Elgamal encryption algorithm and hash function are used for encryption of forwarded data. It is applicable for both sender and receiver to use the same.

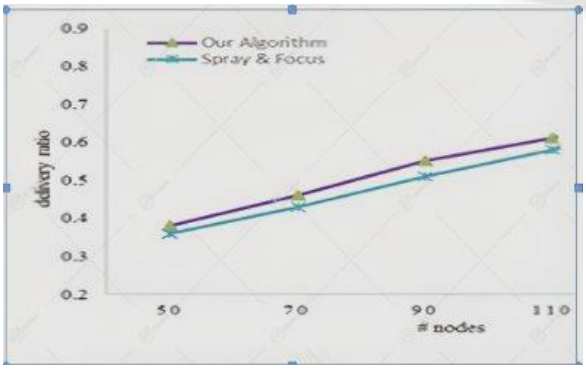

Figure-4: Delivery Vs Node

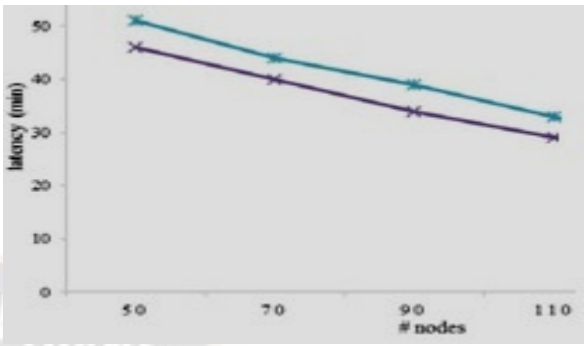

Figure-5: Network latency vs Nodes

VII. CONCLUSION

This research work has concentrated on addressing specific security issues of opportunistic networks. In order to prevent unauthenticated nodes from joining and participating in an opportunistic network this provided a technique for preserving data privacy and location privacy as well. We examined the efficacy of the proposed method on *one simulator*, and the simulation shows that the proposed mechanism performs better in terms of delivery ratio and network latency.

REFERENCES

[1]. Z. Y. Le, G. Vakde, and M. Wright, "Peon: privacy enhanced opportunistic networks with applications in assistive environments, "in Proceedings of the 2nd international conference on Pervasive technologies related to assistive environments, vol. 1–8, Corfu,Greece,June2009.

[2]. W.-C. Kuo, H.-J. Wei, and J.-C. Cheng, "An efficient and secure anonymous mobility network authentication scheme," journal of information security and applications, vol.19,no. 1,pp. 18–24, 2014.

[3]. N. Ahmad, H. Cruickshank, Y. Cao et al., "Privacy by architecture pseudonym framework for delay tolerant network," Future Generation Computer Systems, vol. 93, pp. 979–992,2019.

[4]. C .B. Avoussoukpo, T.B. Ogunseyi, and M.Tchenagnon, "Securing and facilitating communication within opportunistic networks: a holistic survey," IEEE access, vol. 9, pp.55009–55035,2021.

[5]. G. Srivastava, R. Agrawal, K. Singh, R. Tripathi, and K. Naik, "A hierarchical identity based security for delay tolerant networks using lattice based cryptography," Peer-to-Peer Networking and Applications, vol. 13,no.1, pp.348–367,2020.

[6]. K.ChenandH.Shen," FaceChange: attaining neighbor node anonymity in mobile opportunistic social networks with fine

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7209
***Article Received**: 27 April 2023 **Revised:** 15 June 2023 **Accepted:** 29 June 2023*

grained control,"IEEE/ACM Transactions son Networking, vol. 25, no. 2,pp. 1176–1189,2017.

[7]. N.Magaia,C.Borrego, and P.Pereira,"ePRIVO : an enhanced privacy preserving opportunistic routing protocol for vehicular delay-tolerant networks," IEEE Transactions on Vehicular Technology, vol. 67,no. 11,pp. 11154–11168,2018.

[8]. Rashidibajgan,S. & Hupperich,T. Improving the Performance of Opportunistic Networks in Real World Applications Using Machine Learning Techniques. Journal of Sensor andActuatorNetworks11,(2022)

[9]. S. Rashidibajgan, T. Hupperich, R. Doss, and A. F¨orster, "Secure and privacy preserving structure in opportunistic networks,"Computers &Security,vol.104,pp.1–15,2021.

[10]. Rashidibajgan,S.;Doss,R. Privacy preserving history based routing in Opportunistic Networks.Comput. Secur. 2019, 84,244–255.

[11]. Y. Mao, C. Zhou, Y. Ling, and J. Lloret, "An optimized probabilistic delay tolerant network(DTN) routing protocol based on scheduling mechanism for Internet of things (IoT),"Sensors,vol. 19, no. 243,pp.1–16,2019.

[12]. E. K. Wang, Y. Li, Y. Ye, S. M. Yiu and L. C. K. Hui, "A Dynamic Trust Framework for Opportunistic Mobile Social Networks," in IEEE Transactions on Network and Service Management, vol. 15, no. 1, pp. 319-329, March 2018, doi:10.1109/TNSM.2017.2776350.

[13]. Li, F.; Jiang, H.; Wang, Y.; Hashang, L.; Cheng, Y. SEBAR: Social Energy Based Routing scheme for mobile social Delay Tolerant Networks. IEEE Trans. Veh. Technol. 2017, 66,7195–7206.

[14]. Chen,K.;Shen,H.Y.Face Change: Attaining neighbor node anonymity in mobile opportunistic social networks with fine-grained control.IEEE/ACMTrans.Netw.2017,25,1176–118

[15]. Guo,M.,Liaw,H.,Chiu,M.,Tsai,L.: Authenticating with Privacy Protection in Opportunistic Networks Ming Huang.In: EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE2015).pp. 375–380(2015).

[16]. C.Xi,S.Liang, M.Jianfengand, M.Zhuo,"A trust management scheme based on behavior feedback for opportunistic networks," in China Communications, vol. 12, no. 4,pp.117-129, April 2015,doi:10.1109/CC.2015.7114058

[17]. Goyal, M., Chaudhary, M.: Ensuring Privacy in opportunistic Network. IOSR J. Comput.Eng.13, 74–82(2013).

[18]. B.PoonguzharselviandV.Vetriselvi"TrustFrameworkforDataForwardinginOpportunistic network Using Mobile Traces" International Journal of Wireless & Mobile Networks(IJWMN)Vol. 4,No.6, December2012.

[19]. Greede, A. & Allen, Stuart & Whitaker, Roger. (2009). RFP: Repository Based Forwarding Protocol for Opportunistic Networks. Next Generation Mobile Applications, Services andTechnologies,InternationalConferenceon.329-334.10.1109/NGMAST.2009.33.

[20]. Jian Ren, Yun Li, and Tongtong Li, "SPM: Source Privacy for Mobile Ad Hoc Networks",Journal on Wireless Communications and Networking,doi:10.1155/2010/534712,2010.

[21]. A. T. A. Forwarding and S. M. Traces, Data Forwarding In Opportunistic Network Using Mobile Traces, In Data Forwarding In Opportunistic Network Using Mobile Traces, 2012, 425–430.

[22]. M. Alajeely, R. Doss, and A. Ahmad, Security and Trust in Opportunistic Networks – A Survey, IETE Tech. Rev., vol. 33, no. 3, 256–268, 2016.

[23]. J. L. Tsai and N. W. Lo, Provably secure anonymous authentication with batch verification for mobile roaming services, Ad Hoc Networks, vol. 44, 19–31, 2016

[24]. Kang, M.W.; Seo, D.Y.; Chung, Y.W. An efficient delay tolerant networks routing protocol for information-centric networking. Electronics 2020, 9, 839.

[25]. Xiao, Y.; Wu, J. Data transmission and management based on node communication in opportunistic social networks. Symmetry 2020, 12, 1288.

[26]. Goudar, G.; Batabyal, S. Optimizing bulk transfer size and scheduling for efficient buffer management in mobile opportunistic networks. IEEE Trans. Mob. Comput. 2021, 1–16.

[27]. Kandhoul, N.; Dhurandher, S.K. An efficient and secure data forwarding mechanism for opportunistic IoT. Wirel. Pers. Commun. 2021, 118, 217–237.