DETECTION OF MALEVOLENT ATTACK USING DELAY TOLERANT NETWORK DURING POST DISASTER

Abstract

To establish communication in post disaster scenario is a challenging task. Disaster can diminish existing network partially or totally. Smart phone based delay tolerant network (DTN) can help to start communication between nodes in multi hop way. DTN can work in short range communication as with Bluetooth or WIFI connectivity. All the ground nodes can be connected in this way. However, to determine routes in the entire disaster area is more challenging with smart phone based nodes only. We need some Unmanned Aerial Vehicle (UAV) nodes for faster message delivery. Using UAV nodes it is easier to find out routes in disaster scenario than with smart phone based nodes. So, we use some UAV nodes in air communication and coordinate them to deliver messages to ground smart phone based nodes. We use some monitor nodes to track UAV nodes and smart phone based ground nodes. Monitor nodes can find out different malevolent attacks in the network. The malevolent nodes can hamper overall delivery of the network by dropping messages or channelize messages in different route so that they can reach destination in no way. In this paper, we develop some technique to identify malevolent nodes and avoid them during message delivery. Delivery probability is improved in this approach. After the simulation is completed, residual energy still available to continue the simulation further. Simulation is done using Opportunistic Network Environment (ONE) simulator.

Keywords: Malevolent Nodes, Post Disaster Communication, Delay Tolerant Network, Unmanned Aerial Vehicle (UAV), Multi-hop communication, Authentication;

Authors

Chakrabarti Chandrima
Associate Professor,
Department of Computer Science and Engineering Data Science,
Narula Institute of Technology,
Agarpara,Kolkata-109, W.B, India
chandrima.chakrabarti@nit.ac.in

Bal Saptarshi
B.TECH Student,
Department of Computer Science and Engineering, Narula Institute of Technology,
Agarpara,Kolkata-109, W.B, India
saptarshibal16

Jaiswal Rishabh
B.TECH Student,
Department of Computer Science and Engineering, Narula Institute of Technology,
Agarpara,Kolkata-109, W.B, India
rishabhjaiswal2002.rj

Ansari Arbaz Akhtar
B.TECH Student,
Department of Computer Science and Engineering, Narula Institute of Technology,
Agarpara,Kolkata-109, W.B, India
arbazakhtaransari198}@gmail.com

I. INTRODUCTION

Delay Tolerant Network (DTN) is used in post-disaster environment where infrastructure is unavailable [1-3]. Each DTN node can act as router and can collaborate with each other without a central control. There is no predetermined route from the sender to the receiver node; hence, delay is permissible in message delivery [4-5]. Store-carry-forward mechanism is used in multi-hop message forwarding as destination may not be always available in receiving messages. DTN is commonly used in space, remote regions, emergency situations, and catastrophic events where a fixed network is unavailable or inaccessible that we found in Uttarakhand disaster in India in 2021. We here implement Unmanned Aerial Vehicle (UAV) nodes in disaster scenario to introduce faster and smoother message delivery. All ground nodes are connected via Bluetooth or WIFI. Messages can be delivered using smart phone based DTN with maximum delay. This delay can be minimized if we use UAV nodes in message delivery. In post disaster situation routes cannot be determined always. Using UAV nodes it is easier to find out routes in disaster scenario than with smart phone based nodes. So, we use some UAV nodes in air communication and coordinate them to deliver messages to ground smart phone based nodes. Some UAV nodes can eavesdrop messages or even drop messages randomly. We use some monitor nodes to track UAV nodes and smart phone based ground nodes. Monitor nodes can find out different malevolent attacks in the network [6-7]. The malevolent nodes can hamper overall delivery of the network by dropping messages or channelize messages in different route so that they can reach destination in no way. In this proposed work, we develop some techniques to identify malevolent nodes and avoid them during message delivery. Simulation is done using Opportunistic Network Environment (ONE) simulator.

II. RELATED WORK

In UAV self-organizing networks, DTN is mostly used [8]. However, the current UAV self-organizing network routing protocol ignores the prevention of malicious nodes, which could lead to significant security issues, and instead only focuses on increasing message delivery rate, decreasing delivery delay, reducing node energy consumption, and extending network lifetime. In addition to effectively forwarding messages, a secure routing protocol must guarantee message security while it is being transmitted from the source to the destination.

To guarantee the security of data transmission, Asokan et al. [9] suggested using end-to-end data encryption technology. Data encryption, however, is only able to shield the system from message interception; it is unable to stop malevolent attackers, particularly those who gain access to the network through compromised network nodes, from taking down the entire network. To find malicious nodes, Watchdog MDS [10] and CONFIDANT [11] integrate neighbourhood detection with trust. Nevertheless, since the DTN’s feature cannot guarantee an end-to-end connection, it is not feasible to constantly observe neighbours.

A distributed, provenance-aware model called UAV-pro was proposed by Ge et al. [12]. With this approach, peer-to-peer trust evaluation is implemented, and in resource-constrained network situations, the delivery of accurate messages received by destination nodes is maximised while message delay and communication cost are minimised. The history of message ownership that is communicated over a network is referred to as provenance. Based on message integrity, the creators' and operators' actions can be efficiently assessed, leading to the production of observable data. The authors first gather observational data for distributed trust assessment, after which they pinpoint and isolate network's malevolent nodes.

In DTN nodes move differently, so, monitoring can be fairly difficult. In DTN, a malicious node is a node that, like a malevolent node in space, takes any incoming message or data and just forwards it without hesitation. If this data loss occurs in the middle of a crisis, it could negatively impact the entire network architecture. Therefore, identifying malicious nodes and adopting appropriate measures to reduce their impact throughout the adhoc architecture are essential to DTN's functionality.

The authors of [13-15], examine a hybrid attack, whereby attackers are able to simultaneously perform replay, tamper, and packet drop attacks. They employ the data exchange between nodes to assess each node's trustworthiness. Next, nodes are classified as benign or malicious using K-Means clustering. The authors of [16] examine a more sophisticated assault in which malevolent nodes exclusively use data packets delivered to particular neighbour nodes to initiate the aforementioned hybrid attack. They apply the support vector machine (SVM) approach to identify malicious edges, further verifying harmful nodes, and reduce the reputation model of all nodes and edges to a multiple linear regression issue.

An intelligent attack strategy is presented in [17], wherein adversaries execute the hybrid attack exclusively on data packets meeting specific criteria. Algorithms for clustering and regression are used to assess nodes' reliability and separate harmful from benign nodes.
For authentication and security, all of these works presuppose the existence of a centralised security infrastructure. But one cannot presume that such infrastructure will remain operational following a calamity [18–21]. Here, we strive to remove the need of such centralised entities at runtime to address authentication and other security issues [22–26] in a distributed and decentralised fashion. Using as little power as possible is essential when creating ad hoc networks between mobile devices because battery resources are limited.

After getting motivated from this related works, we design a scheme to detect and avoid malevolent attacks in DTN.

III. SYSTEM MODEL

The proposed technique named "Detection of Malevolent Attacks Using Delay-Tolerant Network" aims to enhance communication security within DTNs in post-disaster settings. We have developed the system in post disaster scenario. In post disaster scenario there is no existing infrastructure and network connectivity. So, we use Delay Tolerant Network (DTN) for creating connectivity among nodes. Here, we use, smart phone based node as ground node and UAV nodes as flying nodes. UAV nodes can communicate with each other and send all information to the nearest ground node. Some volunteers may act as ground nodes and some other volunteers can work as UAV controller nodes. So, volunteer nodes can be either ground nodes or UAV controller nodes. However, this type of volunteer nodes can do some malevolent activities, like eavesdrop, drop, and channelize messages to another route and so on. If volunteer nodes will do this kind of malevolent activities, they can be treated as malevolent nodes.

In this work we have implemented schemes for detection of reliable node and malevolent node. Suppose a node wants to forward messages to next hop node for delivering messages towards destination. The node should know the status of its next hop node, either reliable or malevolent. So, we use some monitor node who will detect these different types of node, either reliable or malevolent. We have developed Algorithms 1, 2 and 3 for that.

Figure 1 depicts the proposed system architecture where necessary nodes are arranged to implement post disaster scenario.

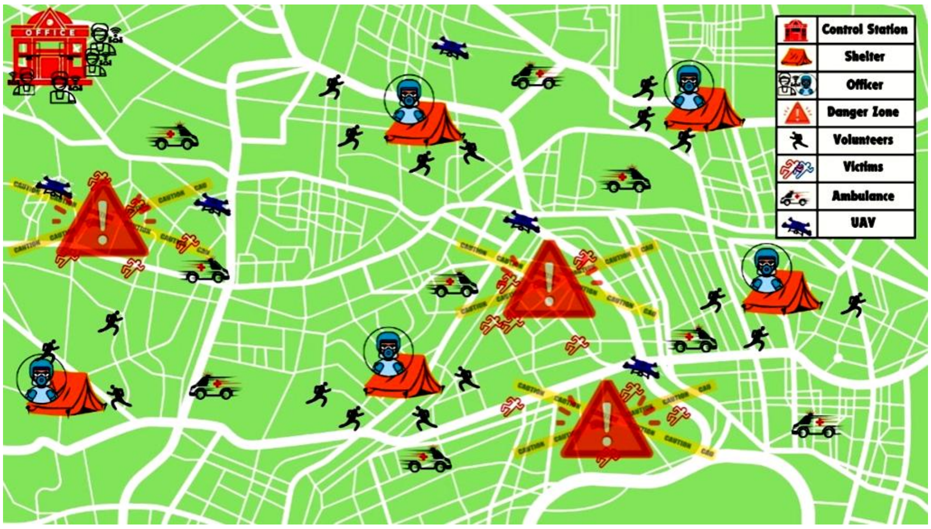

Figure 1: Proposed System Architecture

The system architecture depicted in Figure 1 illustrates that the entire scenario is managed by a main control station located in a city. Officers are the monitors who give volunteers in the post-disaster scenario instructions on how to do their duties. In system architecture there are some entities like, Control Station, Shelter, Volunteer nodes (with Smartphone), UAV volunteer nodes, medical officers, ambulances etc. In order to stabilise the situation and save the casualties, the medical officers and the ambulances also rely on the judgements and directives of the officials from the central control station. We consider control station and shelter nodes are trustworthy. They can authenticate other nodes time to time. Those authenticated nodes can perform communication throughout the network. Unauthenticated nodes cannot participate in communication. Officers can monitor different volunteer nodes activities and classify them as reliable node or malevolent node using Algorithm 1, 2 and 3.

Algorithm 1: Searching for Neighbours

- Start.
- Send “Hello “packets to all ground nodes and UAV nodes within transmission range
- Initialize all routing tables of nodes
- Find neighbours from routing tables as ground nodes and UAV nodes
- Select reliable forwarder nodes using algorithm 2.
- Send messages to reliable forwarder.
- If reliable forwarder node cannot be found
- Wait and set a time limit

- If time limit reached then go to step 2
- Else, choose a new forwarder node from routing table based on destination's reachability
- 11. Set it as reliable forwarder & continue step 6
- 12. Stop.

The algorithm1first sends "Hello" packets to all ground nodes and UAV nodes within their transmission range. Then initialization of routing tables is done for all nodes. Based on "Hello" packets exchange, routing table are updated each time. A node can find its next hop neighbour based on the information in routing table. Neighbours can be found as ground nodes and UAV nodes. Reliable forwarder node can be chosen using algorithm 2. Then messages can be sent via reliable forwarder nodes. If reliable forwarder node cannot be found then each node has to wait for a fixed time limit. If time limit is reached then, each node will choose a new forwarder node from its routing table based on destination's reachability. Finally set that new node as reliable forwarder node and update this process regularly.

Algorithm 2: Detect reliable Forwarder Nodes & Malevolent Node

- Start.
- Initialize monitor nodes as reliable nodes
- Check routing table of all nodes by monitor nodes.
- Identify common routes
- Trace the delivery of messages using common routes to common destination Ncd
- If the common destination (Ncd) is same as exact destination (Nd); If Ncd==Nd
- Common destination node Ncd is reliable node
- Else, common destination (Ncd) is Malevolent node
- Avoid Malevolent nodes and use Reliable nodes in message forwarding
- Stop.

The algorithm2 starts by initialising monitor nodes as reliable nodes, which are then used to check all nodes' routing tables. It identifies common routes to destination. Then delivered messages' routes can be traced to find common destination and common hops. If the common destination is same as exact destination, then it is confirmed that the common destination and common hops are reliable nodes. Else, we can assume that the common destination node and common hops are malevolent nodes.

Hence, we can conclude that malevolent nodes can be avoided and reliable nodes can be chosen as forwarder nodes.

Algorithm 3: Reason for Being Malevolent Node

- Start.
- Find neighbours within communication range.
- If not found then message can't be forwarded.
- 4.Use routing table to find common destination
- If all common destination == Exact destination
- The node is Reliable node

- Else, the node is Malevolent node
- If no neighbours found as Reliable node within time limit
- Select any node as current forwarder node
- If the current forwarder node is malevolent, then the route becomes unreliable.
- Stop.

The algorithm3starts by finding neighbours within communication range. If no node is found then messages cannot be forwarded. Then routing tables can be used to find common destination. If the entire common destination is same as exact destination, then treat the common destination node and common hops are as reliable node. On the other hand, if common destination is different from exact destination, treat all the common destination and common route as malevolent nodes. If no neighbours found as reliable node within time limit, select any node from routing table as forwarder node. If the current forwarder node is malevolent then the route becomes unreliable. We can conclude that, our algorithms can detect reliable nodes and malevolent nodes and also avoid malevolent nodes.

IV. RESULT EVALUATION

In this paper, we have developed a scheme to detect reliable node and malevolent nodes based on their activities like message drop, delay, delivery, overhead. We also monitor if a node has channelized message to other route or not. Analysis is also done on the secure message's overhead ratio, average delay, and delivery likelihood. Additionally, reports on energy levels are produced using various movement models and nodes. Ultimately, we can assure that all nodes are exchanging messages using reliable nodes. In the first simulation scenario, three shelters, three volunteer groups, and three victim groups are taken. This node group has handled the post-disaster management in this case. With the Opportunistic Network Environment (ONE) simulator, we can now assess the outcome of a simulation [27]. The simulation takes 43200 seconds to complete.
Here the following simulation parameters are used.

Table 1: Simulation parameter

Table 1. Simulation parameter	
Simulation time	43200s
Routing	Spray And Wait, Epidemic, Prophet, Max Prop, Energy Aware Router
Movement model	Shortest Path Map Based Movement
No of Control station	1
No of shelters	5
No of volunteers	5 groups, each group has 10 volunteers
No of victims	5 groups, each group has 20 victims

1. Delivery Probability

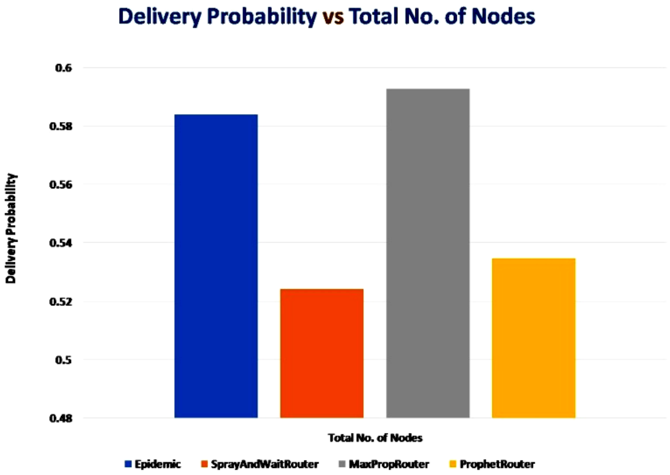

Figure 2: Delivery Probability

We have plotted Time in X axis and Delivery Probability in Y axis. The Spray And Wait Router has provided the highest delivery probability for the Shortest Path Map Based Movement (figure 2), Maximum delivery probabilities ensure efficient and successful delivery of messages to destination. To increase the probability of delivery, use Spray and Wait Router in conjunction with Shortest Path Map Based Movement can be used as highest preference.

2. Latency Average

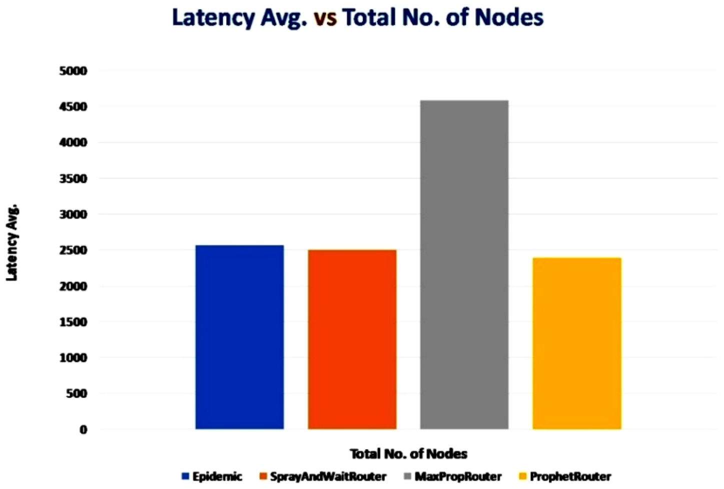

Figure 3: Average latency using different router

Figure 3 depicts time on the X-axis and the latency average on the Y-axis. Spray And Wait Router and Shortest Path Map Based Movement share an excessive delay average. The lowest average latency ensures effective and successful node-to-node communication. To achieve the lowest latency, we need to use Max Prop Router in conjunction with Shortest Path Map Based Movement.

3. Overhead Ratio

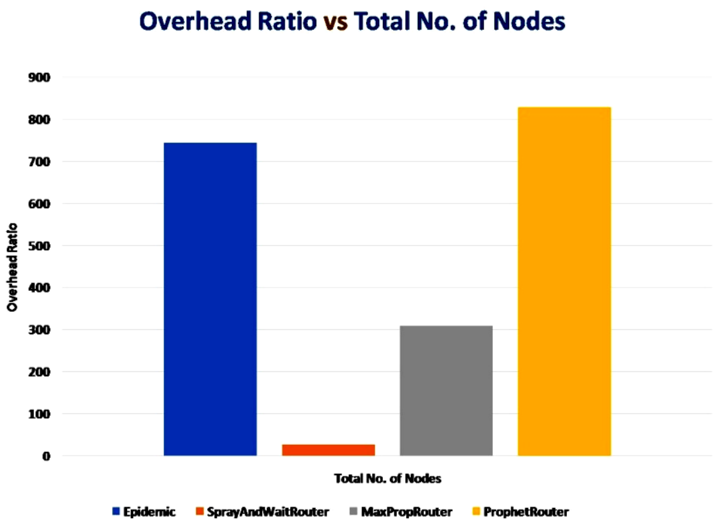

Figure 4: Overhead ratio using different router

Figure 4 plots the overhead ratio as the Y-axis and time as the X-axis. Epidemic Router and Shortest Path Map Based Movement have the highest overhead ratios. Lower overhead ratios ensure more effective and superior communication between nodes, while higher overhead ratios ensure less efficient communication. To achieve the lowest overhead ratio, we need to use spray and wait router in conjunction with shortest path map based movement.

4. Energy Calculation

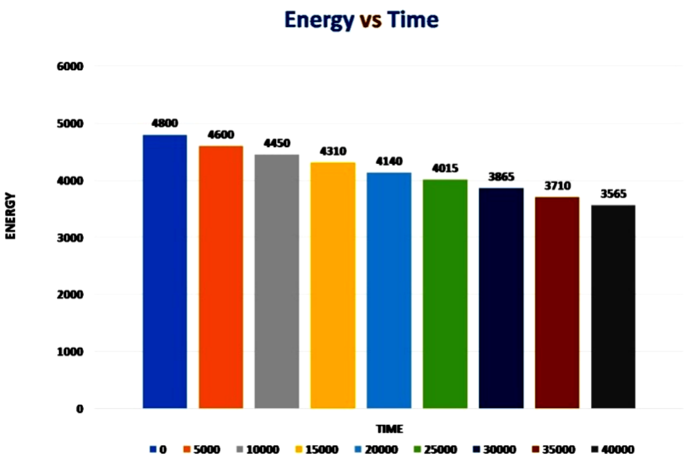

Figure 5: Energy calculation according to time

The X-axis in Figure 5 represents time, while the Y-axis represents energy. The energy consumption of the nodes varies over time. Every node starts with 4800 J energy, i.e same initial energy of all nodes. Following that, the average energy reached 3580 after 43200 seconds. Here, energy spent is minimum, so, we can conclude that our scheme is energy efficient.

5. Percentage of Malevolent Nodes in Different Router

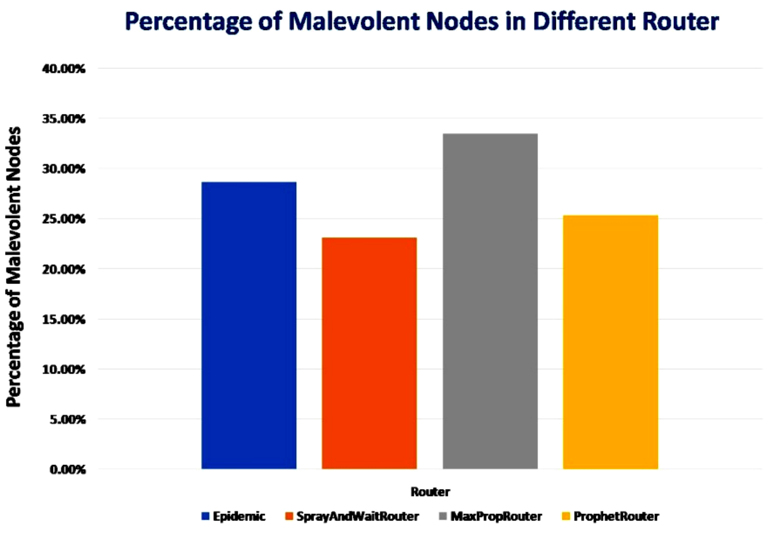

Figure 6: Percentage of Malevolent Nodes in Different Router

The percentage of malevolent nodes among the 166 total nodes is computed in Figure 6. We then compare the proportion for each routing protocol. Using spray and wait router minimum malevolent nodes are associated. So, spray and wait router is the best router to be used in the post disaster scenario where minimum malevolent nodes can work. So, system's performance will be efficient compared to other routers.

V. CONCLUSION

The combination of verification and report allows malicious nodes to be suitably discovered and identified at every stage of the data transmission process. Therefore, we are able to prevent hostile behaviour on the network or remove it by recognising malevolent nodes. In the absence of a hostile actor, we see a considerable decrease in delivery probability and a slight rise in latency and overhead. Therefore, by applying the proposed method, we are able to conclude that the DTN infrastructure is both drastically reduced and significantly affected by hostile nodes. As hostile nodes significantly diminish the network delivery probability, which is the most important factor in a post-disaster scenario, we will address ways to prevent malevolent attacks in the future on the delay tolerant network.AI based detection can be implemented to reduce the overhead of the network.

DECLARATION

The facts and views in the manuscript are ours and we are totally responsible for authenticity, validity and originality etc. We undertake and agree that the manuscripts submitted to your journal have not been published elsewhere and have not been simultaneously submitted to other journals. We also declare that manuscripts are our original work and we have not copied from anywhere else. There is no plagiarism in our manuscripts. Our manuscripts whether accepted or rejected will be property of the publisher of the journal and all the copyrights will be with the publisher of the journal.

REFERENCES

[1] Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004), Security in mobile ad hoc networks: challenges and solutions. IEEE wireless communications, 11(1), 38-47, 2004.

[2] Chakrabarti, Chandrima, and Samir Pramanick, Implementing data security in delay tolerant network in post-disaster management. In Computational Advancement in Communication, Circuits and Systems: Proceedings of 3rd ICCACCS 2020, pp. 77-92. Springer Singapore, 2022.

[3] Garg, Nishu, and R. P. Mahapatra, DTN Security Issues. IJCSNS International Journal of Computer Science and Network Security 9 (8), 2009.

[4] Gohil Tushar Er., Overview of Security Threats in Mobile Ad-hoc Network, Journal of High Performance Communication Systems and Networking Volume. 2 (1-2), pp. 1–10, 2010.

[5] Burg, Adam, Ad-hoc network specific attacks. In Seminar Ad-hoc network, Technische Universities Muenchen, 2003.

[6] BouamS, Othman BJ, Data Security in Ad hoc Networks using Multipath Routing, in Proc. of the 14th IEEE PIMRC, pp. 1331-1335, 2003.
Bouam, Souheila, and Jalel Ben-Othman, Data security in ad hoc networks using multipath routing. In 14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, PIMRC 2003, and vol. 2, pp. 1331-1335. IEEE, 2003.

[7] Hakrabarti, Chandrima, iCredit: A credit based incentive scheme to combat double spending in post-disaster peer-to-peer opportunistic communication over delay tolerant network. Wireless Personal Communications, 121 (3), 2407-2440, 2021.

[8] Giannini, Colian, Ali Alsheikh Shaaban, Chiara Buratti, and Roberto Verdone, Delay Tolerant Networking for smart city through drones. In 2016 International Symposium on Wireless Communication Systems (ISWCS), pp. 603-607. IEEE, 2016.

[9] Asokan, N, Kostiainen, K, Ginzboorg, P, Ott, J, C. Luo, C, Applicability of identity-based cryptography for disruption-tolerant networking, in Proc. 1st Int. MobiSys Workshop Mobile Opportunistic New., pp. 52–56, 2007.

[10] Marti, S, Giuli, T. J, Lai, K, Baker,M, Mitigating routing miss behavior in mobile ad hoc networks, in Proc. 6th Annu. Int. Conf. Mobile Computer. New. pp. 255–265, 2000.

[11] Buchegger, S, Boudec J, Performance analysis of the confidant protocol, in Proc. 3rd ACM Int. Symp. Mobile AD Hoc Netw.Comput. pp. 226–236, 2002.

[12] Ge C, Zhou L, Hancke G, Su, C, A Provenance-Aware Distributed Trust Model for Resilient Unmanned Aerial Vehicle Networks, IEEE INTERNET OF THINGS JOURNAL, VOL. 8(16), pp. 12481-12489, 2021.

[13] Z. Ma, L. Liu, W. Meng, Adaptive detection of malicious nodes under mix-energy-depleting attacks using edge learning in IoT networks, in Information Security, 23rd International Conference, ISC2020, Bali, Indonesia, Proceedings. Springer, pp. 255–273, 2020.

[14] L. Liu, Z. Ma, and W. Meng, Detection of multiple-mix-attack malicious nodes using perception-based trust in IoT networks, Future General .Computer. Syst., vol. 101, pp. 865–879, 2019.

[15] [15] Z. Ma, L. Liu, and W. Meng, towards multiple-mix-attack detection via consensus-based trust management in IoT networks, Computer. Secur. vol. 96, Art. No. 101898, 2020.

[16] L. Yang, L. Liu, Z. Ma, and Y. Ding, Detection of selective-edge packet attack based on edge reputation in IoT networks, Computer. New. vol. 188, Art. No. 107842, 2021.

[17] L. Liu, X. Xu, Y. Liu, Z. Ma, and J. Peng, A detection framework against CPMA attack based on trust evaluation and machine learning in IoT network, IEEE Internet Things J., vol. 8(20), pp. 15249–15258, 2021.

[18] Chakrabarti, C., Roy, S., Adapting Mobility of Observers for Quick Reputation Assignment in a Sparse Post-Disaster Communication Network, AIMoC 2015, Kolkata, India, IEEE proc. pp. 29-35, 2015.

[19] Chakrabarti, C., Roy, S., & Basu, S. Intention aware miss behaviour detection for post-disaster opportunistic communication over peer-to-peer DTN. Peer-to-Peer networking and Applications, vol: 12, 705-723, 2019.

[20] Chakrabarti, C., Basu S., A Blockchain Based Incentive Scheme for Post-disaster Opportunistic Communication over DTN, In Proceedings of ICDCN 2019, ACM, New York, NY, USA, pp. 385-388, 2019.

[21] Chakrabarti, C., Roy, S., iSecure: Imperceptible and Secure Peer-to-peer Communication of Post-disaster Situational Data over Opportunistic DTN, In Proceedings of ICDCN 2019, ACM, New York, NY, USA, pp. 465-468, 2019.

[22] Wang, Haozhen, Xinyu Huang, and Yuanming Wu. GD3N: Adaptive clustering-based detection of selective forwarding attacks in WSNs under variable harsh environments." Information Sciences 665: 120375, 2024.

[23] Tomic, Slavisa, and Marko Beko. Trustworthy Target Localization via ADMM in the Presence of Malicious Nodes. IEEE Transactions on Vehicular Technology, 73(5), 7250-7261, 2024.

[24] Khalid, W., Ahmed, N., Khan, S., Ullah, Z. and Javed, Y., Simulative survey of flooding attacks in intermittently connected vehicular delay tolerant networks. IEEE Access, 11, pp.75628-75656, 2023.

[25] Wenbin Zhai, Liang Liu, Youwei Ding, Shanshan Sun, Ying Gu, ETD, An Efficient Time Delay attack Detection Framework for UAV Networks. IEEE Transactions on Information Forensics and Security, VOL. 18, 2023.

[26] Xu, Jianwen, Kaoru Ota, and Mianxiong Dong. Ideas in the Air: Unmanned Aerial Semantic Communication for Post-Disaster Scenarios. IEEE Wireless Communications Letters, 2025.

[27] Keranen, A., Ott, J. and Karkkainen, T., the ONE Simulator for DTN Protocol Evaluation. In Proceedings of SIMUTools 2009, Article No. 55, 2009.