THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Issue-41-December-2019

An Empirical Study on Security Issues and Mitigation Techniques in Opportunistic Networks

V. Swathi, K. Sumedha and S. Sunitha

Assistsant Professor, SIET, Hyderabad

ABSTRACT

Opportunistic networks is a new and fast emerging paradigm, spontaneously formed by mobile devices equipped with short range wireless technologies such as Bluetooth, WiMax, and can communicate with other devices with in short range. Unlike other delay tolerant networks such as mobile Adhoc networks, nodes in opportunistic networks follow Store, Carry and Forward mechanism to enable communication with other nodes. Further, a fixed path between the source and destination never exists. Neighbor discovery, connection establishment and data dissemination are challenging tasks in these networks due to frequent disruption of communication links and topology changes. The characteristics of these networks are high mobility of nodes, limited power, low density and long communication delays. These nodes suffer from different kinds of attacks by suspicious nodes making them more complex and challenging networks. Security issues such as confidentiality of data, routing security, cooperation, non-repudiation, access control, availability, authentication and trust management are to be exclusively addressed so as make these networks reliable. This paper discusses various routing protocols in opportunistic networks, types of security attacks, their mitigation strategies and the necessity of further enhancements.

Index Terms: Opportunistic Networks, store-carry-forward, delay tolerant networks, data dissemination, security issues.

I. INTRODUCTION

Opportunistic networks are a type of delay tolerant networks [1] and are also called as intermittently connected networks as a fixed path between the source and destination nodes does not exist and these links are often subject to disruption. Opportunistic networks are Self-organizing infrastructure less Mobile networks where routes are built dynamically and the process of exchanging and forwarding of messages is done in a node-by-node manner basing on the forwarding opportunities that exist in the network. The nodes store data for longer time and forward it only to the best node available which has the maximum probability of forwarding the message to the destination using store, carryand forward paradigm.

People carrying mobile devices (such as mobile phones, personal computers, PDA etc.,) enable spontaneous formation of opportunistic networks as these devices are equipped with wireless technologies such as WiMax, Bluetooth etc. [2], that communicate with nodes with in short distance without relying on any fixed network topology. The characteristics of opportunistic networks such as high mobility of nodes, frequent link disruption, limited power, low density, long communication delays, no end-to-end connectivity, etc make these networks more challenging and unique from other delay tolerant networks such as MANETS.

In MANETS a fixed communication link is established for forwarding of messages through the intermediate nodes. Unlike MANETS message passing in opportunistic networks is through the opportunistic contacts established among the mobile nodes, where a fixed message routing path is not available. Nodes in Opportunistic networks, without possessing or acquiring any information about the network topology, exhibit a One-hop wireless message communication scheme, where the exchange of messages is only between the directly connected nodes. The nodes in Opportunistic networks include heterogeneous wireless communication devices like Wi-Fi, Bluetooth, satellite communication etc. [2].

The mobility of nodes creates contact opportunities between the nodes that are otherwise disconnected. Figure 1 shows the contact opportunities established through node mobility between the source S and destination D nodes in Opportunistic networks. The communication link between the source and destination nodes is not a direct path at any time. Data is delivered from source to destination via the intermediary nodes

ISSN:0971-1260

Vol-22-Issue-41-December-2019

using store, carry and forward mechanism. In Figure 1(a) at time t1, the source node identifies node 1 as the nearest node and forwards the message; in Figure 1(b) at t2 > t1, node 1 chooses node 3 and forwards the packet; in Figure 1(c) at t3>t2 node 3 chooses node 4 and forwards the message to node 4 and in Figure 1(d) at t4 > t3, node 4 forwards the packet to node D.

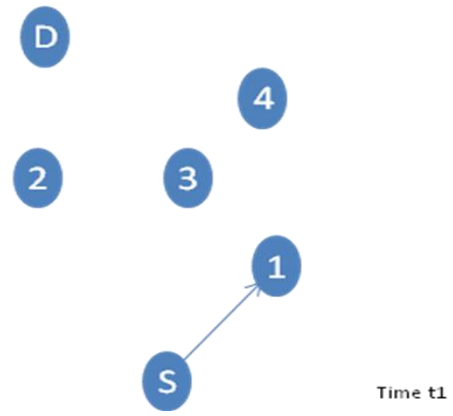

Figure 1(a)

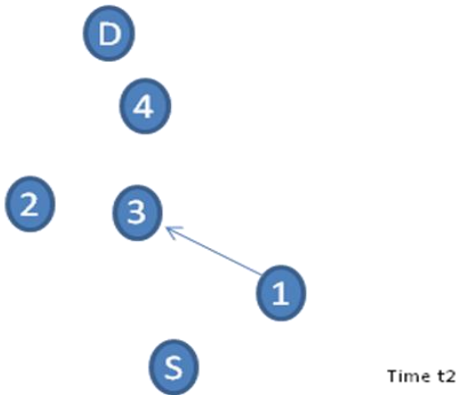

Figure 1(b)

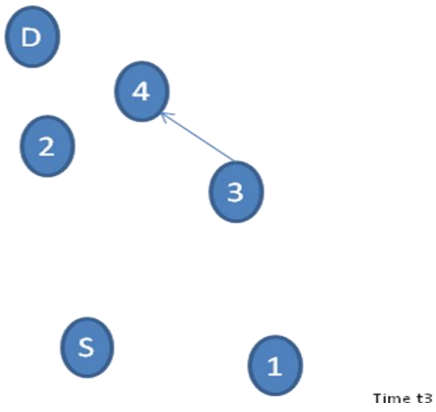

Figure 1(c)

ISSN:0971-1260

Vol-22-Issue-41-December-2019

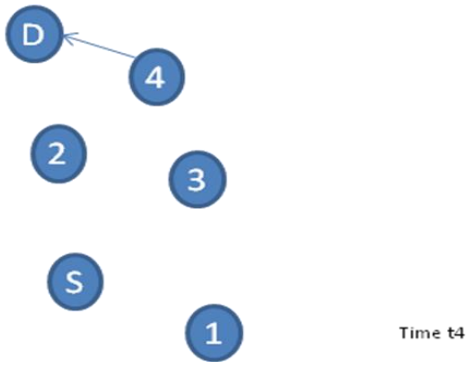

Figure 1(d)

Figure 1(a), (b), (c), (d): Taxonomy of Opportunistic routing due to node mobility

II. APPLICATION AREAS OF OPPORTUNISTIC NETWORKS

The application areas of Opportunistic networks are the places with lack of communication infrastructure, bad network environment and emergency incidents. As a new networking paradigm, Opportunistic networks application areas [2] include, Zebra Net-wildlife areas to track animal migration, emergency situations, Search and Rescue systems, under water projects. Other Diverse Applications include Agriculture, Environment, Healthcare, Manufacturing, Surveillance, and Transportation.

This paper, provides an outline of the routing and data dissemination methods, Vulnerabilities and security issues in Opportunistic Networks and current approaches that mitigate these issues.

III. ROUTING PROTOCOLS

The traditional Routing protocols cannot be applied to Opportunistic networks as there is no fixed route between the source and destination nodes. Hop by Hop, messages are forwarded to the destination node with the help of intermediary nodes. It is apparent that, the store, carry and forwarding mechanism to route the messages among the nodes depends up on the contact opportunity that arise as the nodes are mobile [3]. The node holding the data must intelligently take the decision of choosing the next suitable node for forwarding of messages basing on the criteria of the employed protocol [4]. The routing protocol must therefore perform the following functionalities to forward the messages to the next node.

1. Neighbour discovery: A node must identify or discover other nodes in its neighborhood to start collaboration. The collaboration can be an active collaboration in form of user notification or passive collaboration by the execution of a data sharing protocol. A node in the network must be able to discover the other nodes with which a direct communication link can be established.
2. Route establishment and Data dissemination: After neighboring nodes are identified, using the routing algorithms connection is established to disseminate data i.e., Information is distributed among nodes in the network.

Various protocols for routing and data dissemination techniques [5] have been proposed for efficient delivery of data. Figure 2 shows the classification of various routing algorithms in opportunistic networks basing on how data is disseminated to the destination. These algorithms can be broadly classified into two categories as Flooding-based routing approach and Forwarding-based routing approach.

1. Flooding based Routing protocols: These protocols simply flood the data to all the nodes within the contact range. In this way multiple copies of the message are quickly forwarded throughout the network and also have a high probability of reaching their destination. Examples of these protocols include Epidemic Routing [6], Spray and wait [7], Network Coding based routing [8], etc. These protocols incur significant demand on both bandwidth and buffer.

ISSN:0971-1260

Vol-22-Issue-41-December-2019

2. Forwarding based Routing Protocols: - These are Single copy routing protocols, in which the forwarding decisions are made to choose the best next node that has the highest probability of forwarding the data towards the destination.

These forwarding based Protocols are further classified as:-

a) Content based routing protocols: As the name suggests, Content centric networks, request and route data based on the content and is not concerned with the sender or the receiver. They allow the user to focus on the data they want rather than having to specify a location of the data. The content centric approach uses a generic publish/subscribe scheme for data dissemination. Examples of such protocols include PodNet [9], Propicman [10], Content place [11], Repository based data dissemination [12], Interest awareness in data dissemination [13] etc.

b) Context based routing protocols: Context-based routing protocols identify the next suitable hops by exploiting the context information on which the nodes are working. Each next hop is selected by considering the utility factor of that node. Each node maintains the utility value obtained by its association with all the other nodes in the network [1]. These techniques reduce messages duplication but increase the delay in delivering the message and the cost to update and hold the utility values at each node is an additional overhead [14].Examples of these protocols include Context-aware routing[15], Moby Space[16] etc.

c) Social-Context based Routing protocols: The method of forwarding the messages by Social–Context based routing protocols is through exploiting the context information and the social contacts of the nodes as a decision parameter. The social contacts of a node are the information related to a group and also its history of social relationships [4]. Examples of these protocols include Bubble Rap [17], HiBop [18], Socio-Aware [19],etc.

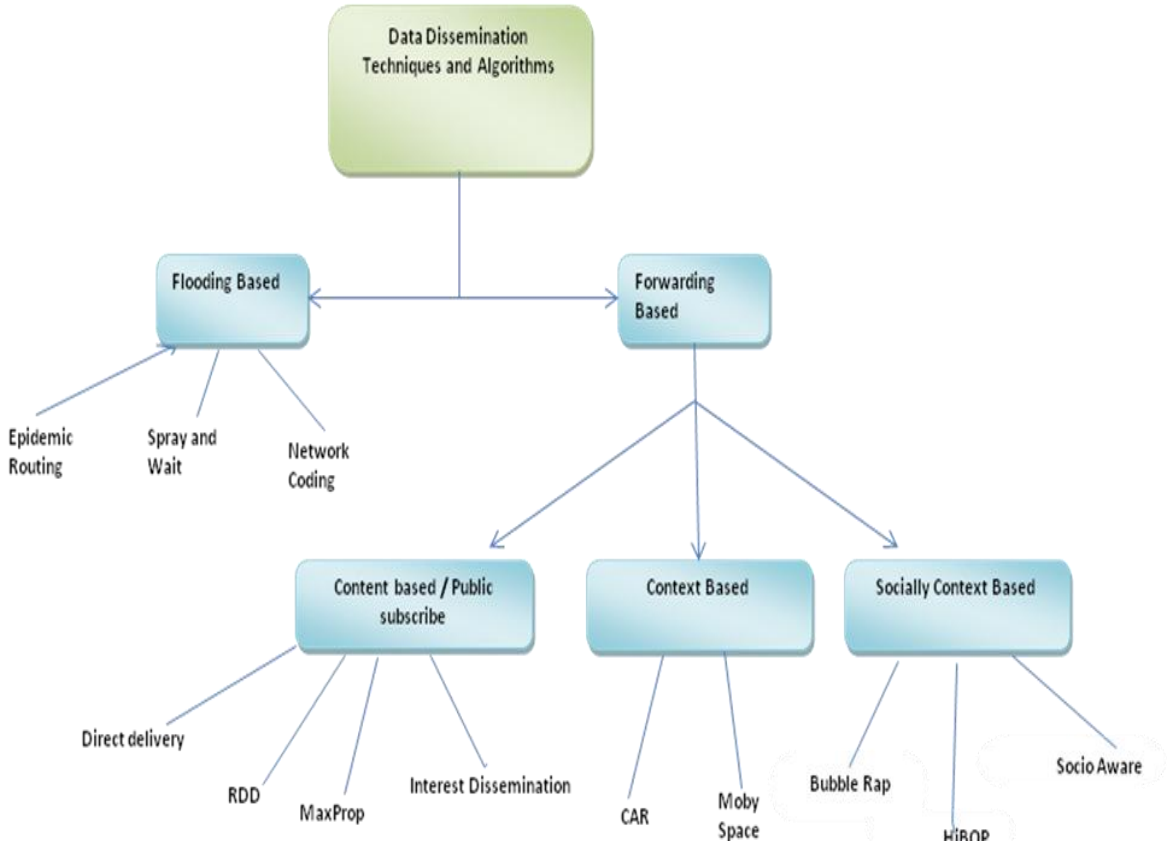

FIGURE 2: CLASSIFICATION OF DATA DISSEMINATION TECHNIQUES AND ALGORITHMS

ISSN:0971-1260

Vol-22-Issue-41-December-2019

IV. VULNERABILITIES IN OPPORTUNISTIC NETWORKS

The characteristics of Opportunistic networks expose them to a number of vulnerabilities making security a serious concern in this type of networks. Following are some of the Vulnerabilities in opportunistic networks:-

1. Unauthorized access:- Due to the absence of centralized management, identifying the attacks from unauthorized access[20]-[21] is very difficult . As the network resources in opportunistic networks are very scarce, unauthorized access to such resources leads to performance degradation of the networks.
2. Confidentiality:- Opportunistic networks follow store,carry and forward mechanism , where data travels through the intermediary nodes, stored, carried and on identifying a suitable node data is forwarded . Data in these networks is highly exposed to possibility of an intermediary node saving a copy of the information or disclosing the information before forwarding. Confidentiality [20] in opportunistic networks must ensure that information cannot be accessed by unauthorized nodes.
3. Integrity:- Integrity[20] in opportunistic networks must ensure that data is not modified or incorrect data is not induced by the intermediate nodes during the data forwarding process.
4. Resources:- The availability of resources[20] such as Storage, Communication link ,Band width, Power Supply etc are limited in these networks and are vulnerable to attacks such as resource depletion attacks.
5. Privacy:- Privacy preservation[20] is a challenging task in these type of networks as the information is often stored in the intermediary nodes . Accessing of Location privacy, Identity privacy, Communication Privacy or other sensitive data by the intermediate nodes pose threat to User privacy .
6. Dynamic Topology:-As a fixed path between the source node and the destination node cannot be established before forwarding the messages and the transfer of these messages is done on a node-by-node basis, identifying malicious nodes, selfish nodes or compromised nodes[22] is difficult in opportunistic networks.
7. Trust and Cooperation:-Nodes in opportunistic networks often join and leave the network and messages are stored in the intermediary nodes, a need for a novel mechanisms that resist the malicious nodes from unauthorized access and ensure trust and cooperation[20] between the nodes is emphasized .
8. No Network boundary:- Due to the mobility of nodes there is no defined physical boundary[23] for these networks and nodes frequently join and leave the network. Whenever a node comes into the radio range of other nodes it will be able to communicate with that node, leading to a number of attacks such as, Message tampering, Impersonation, Denial-of-Service etc.

V. SECURITY ATTACKS IN OPPORTUNISTIC NETWORKS

The characteristics of opportunistic networks emphasize Security as one of the prime concerns. Various Security mechanisms must be enforced to keep the network free from these attacks especially in the areas vulnerable to severe attacks. Attacks in opportunistic networks can be identified as internal attacks and external attacks. Internal attacks are caused by the nodes that are within the same network or part of the domain and these types of attacks have more impact as internal nodes have complete knowledge about the network resources. On the other hand, external attacks are experienced from the nodes outside the network and have less impact on the network as these nodes have inadequate information about the network resources [2]. The following are the various security threats that degrade the performance of opportunistic networks.

1. Sybil attack: - The suspicious node creates a numerous false Ids [2] to establish communication with its neighboring nodes and drops the received packets and the identification of such nodes is also difficult.
2. Packet dropping attack by selfish nodes: - Selfish nodes [24] are the nodes that do not forward messages to another node but uses network services. Due to scarce availability of resources such as battery and storage, nodes behave selfishly and avoid cooperating with other nodes.

ISSN:0971-1260

Vol-22-Issue-41-December-2019

3. Fake packet injecting attack: - This attack is commonly used in Denial of service attacks and man in the middle attacks where an unknown or malicious node tries to inject fake packets in to the network or between the nodes that are communicating, which leads to blockage or degradation of network services. Forged packets [25] are accepted by the nodes as there structure of the message received is formally correct.
4. Black hole attack: - In this attack[2]-[26] the suspicious node announces that it has the best possible route to forward the data to the destination node and when it receives the data from its neighbor it silently drops the packets or discards them without forwarding.
5. Worm hole attack: - In this attack [2] the suspicious node records packets of data at a specific location on the network and forwards these packets to other locations and retransmits them from that locations.

VI. MITIGATION TECHNIQUES

1. Sybil Attack: - In Sybil attack the suspicious node creates numerous false identities and drops the receiving packets [2]. In [27], the defense mechanisms against Sybil attacks are proposed, that validates each node identity either by direct or indirect methods for node validation. In direct method of node validation each node mutually tests whether the other node is valid or not. In indirect method of validation, already verified nodes are allowed to verify the other nodes in the network. In [28], Trusted Certification, RSSI based scheme and incentive based mechanisms are discussed.
2. Packet Dropping Attack: - In this type of attack the suspicious node drops packets intentionally which it receives from the other nodes. Several mechanisms are proposed to detect such type of attacks in the networks. In [24], multipath routing, multipath data forwarding, network coding, ferry based trusted monitoring, anti-localization mechanisms are discussed and also presents a new mechanism in which the intermediate nodes identify the suspicious node that attempts to drop packets instead of source and destination nodes only.
3. Fake packet injecting Attack: - In this type of attack the malicious node tries creates false packets and injects these packets in to the network, which leads degradation of network services. As the structure of these packets is correct the nodes in the network receive these packets. In [25] a node-by-node source authentication scheme is discussed and also a new forwarding mechanism, on-demand and node-by-node source authentication and forwarding (SAF) protocol is proposed for forwarding the packets.
4. Defense against Black hole attacks:- In this attack the suspicious node attracts its neighbor nodes by announcing that it has the best route and when it receives the data from its neighbor it drops the packets without forwarding. In [25] ,mechanisms to defense against black hole attacks such as Packet exchange record mechanism, cluster based detection scheme, ferry based detection method, improved ferry based detection methods are discussed and also a new solution to mitigate black hole attacks using between-ness metric is proposed.
5. Defense against Worm hole attacks: - In this attack the suspicious node redirects the packets to other locations and replays them from that location. In [2], defense mechanisms such as packet leash technique, Geographical leash technique, temporal leash techniques are discussed. A new method for detecting and isolating the worm hole attack which is a modification to the ad hoc on-demand distance vector protocol is also discussed.

VII. CONCLUSION

Opportunistic networks are a type of delay tolerant networks where a fully connected path between source and destination does not exit at any time. They are also referred to as intermittently connected networks where data is forwarded using the use store, carry and forward mechanism on a node-by-node basis until a suitable contact opportunity arises. The characteristics of these networks such as high mobility of nodes, no fixed infrastructure, highly dynamic topology etc exposes them to different types of security risks. Opportunistic networks have a wide a range of applications but also suffer from various vulnerabilities. In this paper an attempt is made to outline the basic concepts in opportunistic networks, various routing and

ISSN:0971-1260

Vol-22-Issue-41-December-2019

data dissemination protocols. Vulnerabilities caused by the characteristics of these networks are briefed along with the various mitigation strategies. Further, the impact of Packet dropping and fake packet injecting attacks in content based data dissemination protocols and the defense mechanisms against these attacks are to be extensively addressed to provide a more secure and reliable networks, protecting them from various internal and external attacks.

REFERENCES

[1] L. Pelusi, A. Passarella, M. Conti, and I. I. T. Cnr, "OpportunisticNetworking : Data Forwarding in Disconnected Mobile Ad Hoc Networks Introduction Realistic Cases Opportunistic Routing Forwarding Techniques," no. November 2006, 2007.

[2] M. Alajeely and R. Doss, "IETE Technical Review Security and Trust in Opportunistic Networks – A Survey Security and Trust in Opportunistic Networks À A Survey," vol. 4602, no. October, 2015.

[3] V. F. S. Mota, F. D. Cunha, D. F. Macedo, J. M. S. Nogueira, and A. A. F. Loureiro, "Protocols , mobility models and tools in opportunistic networks : A survey," vol. 48, pp. 5–19, 2014.

[4] C. Prabha, S. Kumar, and R. Khanna, "Analysis of Routing and Forwarding Protocols in Opportunistic Networks," Procedia Comput. Sci., vol. 85, no. Cms, pp. 891–898, 2016.

[5] Issac Woungang,Sanjay Kumar Dhurander,Alagan Anpalagan,Athanasios V.Vasilakos"Routing in Opportunistic networks",pp 145-178.

[6] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks", Tech. Rep. CS-2000-06, Department of Computer Science, Duke University, Durham, NC, 2000.

[7] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and Wait : An Efficient Routing Scheme for," Direct, pp. 252–259, 2005.

[8] J. Widmer and J.-Y. Le Boudec, "Network coding for efficient communication in extreme networks," Proceeding 2005 ACM SIGCOMM Work. Delay-tolerant Netw. - WDTN '05, pp. 284–291, 2005.

[9] C. Boldrini and A. Passarella, "DATA DISSEMINATION IN OPPORTUNISTIC NETWORKS," pp. 1- 44

[10] S. Giordano, H. A. Nguyen, S. Giordano, and A. Puiatti, "Probabilistic Routing Protocol for Intermittently Connected Mobile Ad hoc Network (PROPICMAN)," no. September, 2015.

[11] C. Boldrini, M. Conti, and A. Passarella, "ContentPlace : Social-aware Data Dissemination in," pp. 203–210.

[12] A. Greede, S. M. Allen, and R. M. Whitaker, "RDD : Repository-based Data Dissemination Protocol For Opportunistic Networks," pp. 101–106, 2012.

[13] R. Ciobanu, R. Marin, C. Dobre, and V. Cristea, "Ad Hoc Networks Interest-awareness in data dissemination for opportunistic networks," Ad Hoc Networks, vol. 25, pp. 330–345, 2015.

[14] C. Boldrini, M. Conti, A. Passarella, and V. G. Moruzzi, "Context and resource awareness in opportunistic network data dissemination," no. 027918, 2008.

[15] M. Musolesi, S. Hailes, and C. Mascolo, "Adaptive Routing for Intermittently Connected Mobile Ad Hoc Networks," IEEE Int. Symp. a World Wirel. Mob. Multimed. Networks, pp. 183–189, 2005.

[16] J. Leguay, T. Friedman, and V. Conan, "Evaluating mobility pattern space routing for DTNs," Proc. - IEEE INFOCOM, 2006.

[17] P. Hui, J. Crowcroft, and E. Yoneki, "BUBBLE Rap : Social-based Forwarding in Delay Tolerant Networks," pp. 241–250, 2008.

ISSN:0971-1260

Vol-22-Issue-41-December-2019

[18] P. Computing, C. Boldrini, I. National, M. Conti, I. National, A. Passarella, and I. National, "Exploiting users ' social relations to forward data in opportunistic networks : The HiBOp solution," no. September 2015, 2008.

[19] P. Costa, C. Mascolo, M. Musolesi, and G. Pietro Picco, "Socially-Aware Routing for Publish-Subscribe in Delay-Tolerant Mobile Ad Hoc Networks," vol. 26, no. 5, pp. 1–13, 2008.

[20] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, "Security and trust management in opportunistic networks: A survey," Secur. Commun. Networks, vol. 8, no. 9, pp. 1812–1827, 2015.

[21] P. Yau and C. J. Mitchell, "Security vulnerabilities in ad hoc networks," Seventh Int. Symp. Commun. Theory Appl. July 13--18, 2003, Ambleside, Lake Dist. UK, pp. 99–104, 2003.

[22] M. Goyal and M. Chaudhary, "Ensuring Privacy in opportunistic Network," IOSR J. Comput. Eng., vol. 13, no. 2, pp. 74–82, 2013.

[23] S. Gotmare and A. Bannore, "Vulnerabilities, Threats and Security Methods in Network Layer of Mobile Adhoc Network : An Overview."

[24] A. Ahmad, M. Alajeely, and R. Doss, "Defense against packet dropping attacks in opportunistic networks," Proc. 2014 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2014, no. August, pp. 1608–1613, 2014.

[25] Q. Gu, "Defense Against Packet Injection in Ad Hoc Networks," pp. 1–27.

[26] A. R. Naseer, S. Member, and A. Saichand, "Mitigating Black Hole Attacks in Opportunistic Routing for Delay Tolerant Networks," vol. I, 2016.

[27] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," Proc. third Int. Symp. Inf. Process. Sens. networks IPSN04, pp. 259–268, 2004.

[28] A. M. Bhise and S. D. Kamble, "Review on Detection and Mitigation of Sybil Attack in the Network," Procedia Comput. Sci., vol. 78, pp. 395–401, 2016.