International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

A Study on Detection and Prevention of Blackhole & Greyhole Attacks in DTN

Labala Sarathchandra Kumar & Dr G Lavanya Devi

M.Tech, Department of CS&SE, College of Engineering, Andhra University, Visakhapatnam.
Assistant Professor, Department of CS&SE, College of Engineering, Andhra University, Visakhapatnam.

Abstract:

Delay Tolerant Network is a network in which there is no end to end connectivity between source and destination. DTN is characterized by long propagation delay and intermittent connectivity. Due to the limited connectivity, DTN is vulnerable to various attacks, including Blackhole and Greyhole attacks. Malicious nodes drops all or a part of the received messages, even if they have enough buffer storage. This dropping behaviour is known as Blackhole and Greyhole attacks respectively. This paper provides a new scheme and its comparison with different parameters. Existing research scheme can detect individual attackers well but they cannot handle the case where attackers cooperate to avoid the detection. The limitation of previous work is that they cannot defend against collusion attacks. Therefore there is a need to develop new attack detection scheme that detects collusion attacks effectively. Blackhole and Greyhole behaviours represent a serious threat against routing in Delay or Disruption Tolerant Networks. Due to the unique network characteristics, designing a misbehaviour detection scheme in DTN represents a great challenge. DTN assume that network nodes voluntary cooperate in order to work properly. This cooperation is a cost intensive activity and some nodes can refuse to cooperate, leading to a selfish node behaviour. Normally nodes are required to exchange their encounter data, in which malicious nodes intentionally drop all or part of it. Thus, so the overall network performance could be seriously affected. At the time of use a watchdogs is a well -known mechanism to detect selfish nodes like that trusted authority, relying on local watchdogs alone can lead to poor performance when detecting selfish nodes, in term of precision and speed. This is especially important on networks with sporadic contacts, such as DTNs, where sometimes watchdog's lack of enough time or information to detect the selfish nodes. Thus, we propose Statistical based Detection of Blackhole and Greyhole attackers (SDBG to address both individual and collusion attacks) to detect the individual and colluding misbehaviour nodes and prevent the network from them. Detection of attacker node increases the precision when detecting selfish nodes. Extensive simulation shows that our solution can work with various scenarios and different number of attackers per collusion at high accuracy and less delay.

Keywords

DTN, Black Hole Attack, Grey Hole attack, Security in DTN, Collusion Attacks, Routing in DTN

1. Introduction

In Mobile Ad hoc Network (MANET) packets can be transferred only if link between the nodes are established. If link is not established then packets will be lost. So packet delivery ratio will be decreased in MANET. To overcome this problem, Delay Tolerant Network is used. In DTN each node has some storage capacity. So if the links of nodes are not established then packets will be stored in the storage. DTN is able to provide communication services in unreachable and unfriendly environments. A DTN is a network architecture that defines a series of contiguous network data bundles that enables applications. In DTN, there is no end to end connectivity between source and destination. It is characterized by long propagation delay and intermittent connectivity. DTN is a set of protocols that acts together to enable a standardized method of performing store-carry-forward mechanism. It is developed to cope with intermittent connectivity and long delay in wireless networks. Due to the limited connectivity, DTN is vulnerable to blackhole and greyhole attacks in which malicious nodes intentionally drop all or part of the received messages. Although existing proposals could accurately detect the attack launched by individuals, they fail to tackle the case that malicious nodes cooperate with each other to cheat the defence system. In this paper, we suggest a scheme called Statistical based Detection of Black hole and Grey hole attackers (SDBG) to address both individual and collusion attacks. Nodes are required to exchange their encounter record histories, based on which other nodes can evaluate their forwarding behaviours. To detect the individual misbehaviour, we define forwarding ratio metrics that can distinguish the behaviour of attackers from normal nodes. Malicious

nodes might avoid being detected by colluding to manipulate their forwarding ratio metrics. To continuously drop messages and promote the metrics at the same time, attackers need to create fake encounter records frequently and with high forged numbers of sent messages. We exploit the abnormal pattern of appearance frequency and number of sent messages in fake encounters to design a robust algorithm to detect colluding attackers.

DTN network has the following several characteristics:

1. Long delay
2. Limited resources
3. Intermittent connectivity
4. Asymmetric data rate
5. High error rate
6. No end to end path between source and destination

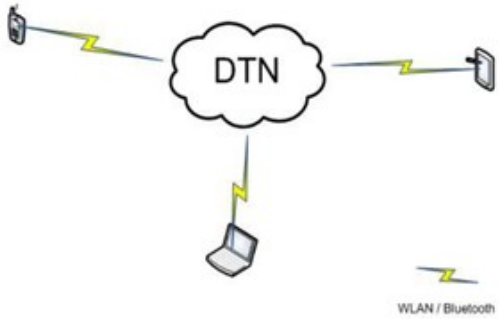


Figure 1: DTN Architecture

2. Application Areas of Delay Tolerant Network

These are following application areas of Delay Tolerant Network

1. Wild Life Monitoring

This application is concerned with gathering data about wild species and their habits. One of the most famous examples of wildlife monitoring is the Zebra NET project conducted in Sweet waters Reserve, Kenya. Here, zebras are equipped with custom tracking collars (nodes) and carried across a large wild area. The collars include GPSs, flash memory, wireless transceivers, and a small CPU.

2. Underwater Sensors

In this application, medium of transmission is water. Radio Frequency communication generally does not work in water. Due to the nature of the location, nodes (mobile or stationary) may experience long partitioning periods before contacting each other or some info-stations. Within the same context of underwater sensing, there is the example of SeaWeb, a project conducted by the U.S. Navy. SeaWeb has developed its own MAC layer protocol, especially optimized for the acoustic networking case. The nodes in the SeaWeb have been mainly disposable in that they run on batteries with no possibility for recharging.

3. Village Network

Rural areas have limitations of lacking of infrastructure. Village networks represent a very promising public application for DTNs, especially in secluded areas lacking communication infrastructure. Rural buses may be also used to provide Internet connectivity to isolated and remote villages. Buses act here as relays or couriers, transmitting and exchanging data via simple wireless transmission across the cities bus network. Like in the Sea Web example, several other connectivity options may be integrated here (e.g. satellites, LEO, GEO, telephones) to aid the delivery process.

4. Interplanetary Network

The massive distances separating terrestrial artificial objects and the need for these objects to exchange data among each other or with base-stations on earth –or perhaps other planets-represent an extreme case of DTN communication. NASA's vision of an Inter-Planetary Network (IPN) that initiated the search for a heterogeneous architecture that overcomes the traditional limitations of TCP, which eventually evolved into the DTN field of research. The combination of long signal propagation times and intermittent connectivity caused by the interposition of a planetary body between the sender and the receiver can result in round-trip communication delays measured not in milliseconds or even minutes but in hours or days.

5. Military Applications

There is a need to monitor extended geographical planes, their objects and inhabitants-i.e. soldiers-who would be equipped with wireless sensors in order to indicate their locations. Battlefields are dangerous. While it would be acceptable to assume human interference in collecting data from the nodes (e.g. an info-station is driven close enough to zebra herds to allow for wireless interaction), it is expected that a higher level of automation is presented in military application. Tactical military networks are established in a very Ad Hoc manner. The nodes are in continuous and rapid motion. And there is most likely no stable infrastructure due since such infrastructure would just provide a target for the enemy.

3. Store-Carry-Forward Mechanism

DTN works on the principle of store-carry and forward mechanism. Delay Tolerant Networks have overcome the problems associated with the conventional protocols using the concept of store-carry and forward method. Under this paradigm, each node in the network stores a packet that has been forwarded to it by another node, carries the packet while moves around, and forward it to other relay nodes or to the destination node when they come within transmission range. DTN nodes utilize store-carry messages can be sent over an existing link and buffered at the next hop until the next link in path appears. It is similar to postal service, every letter has to pass through a set of post offices and here it is processed and forwarded, before reach destination. Here complete

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

message of it is transferred and stored in nodes successively until it reaches the destination.

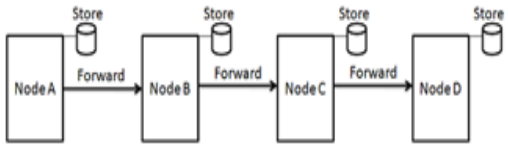


Figure 2: Store-Carry-Forward Mechanism

Blackhole Attacks

Blackhole attackers drop all the received messages even if they have enough buffer storage. Attacker can drop received routing messages, instead of relaying them as the protocol requires, in order reducing the quantity of routing information available to the other nodes. Blackhole Attack is a "passive" and a simple way to perform a Denial of Service. The attack can be done selectively (drop routing packets for a specified destination, a packet every n packets, a packet every t seconds, or a randomly selected portion of the packets) or in bulk (drop all packets), and may have the effect of making the destination node unreachable or downgrade communications in the network.

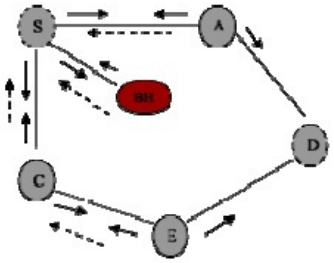


Figure 3: Blackhole Attack

Greyhole Attacks

Greyhole attackers drop a fraction of received messages to avoid arousing suspicion and detection from other nodes. In Greyhole attacks, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it. The dropping misbehaviour will decrease the overall message delivery and waste the resources of intermediate nodes that have carried and forwarded the dropped messages. DTN makes use of hop-by-hop routing and the store-and-forward paradigm to overcome the lack of end-to-end paths.

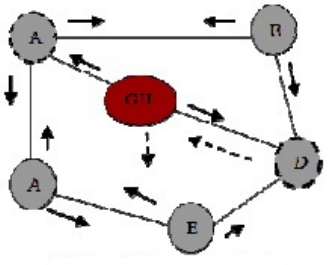


Figure 4: Greyhole Attack

Individual Attacks

An attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of a useful data.

Collusion Attacks

Malicious nodes are cooperate with each other to cheat the defense system called as colluding attackers, who misbehaving with the normal nodes by creating fake records for each other called as collusion attacks.

4. Related Work

Cryptography provides networks with basic security services such as authentication, message integrity and non-repudiation. Several works have focused on designing cryptography schemes suitable in DTN and applying cryptography to the links to secure against malicious nodes. The cryptography approach can protect networks from unauthenticated external adversaries. However, it is not enough to defend against authenticated internal adversaries who launch such attacks as Blackhole and Greyhole attacks. Therefore, researchers have proposed misbehaviour detection schemes to detect and mitigate insider attackers. Several intrusion detection approaches have been proposed for mobile ad hoc networks. Many of the approaches assume that there are sufficient neighbours to help monitor the transmissions and receptions of data packets by other nodes to detect abnormality. However, in a sparsely connected ad hoc network, nodes usually have very small number of neighbours. In addition, new history based routing schemes e.g. Prophet have been proposed because traditional ad hoc routing schemes do not work well in sparse ad hoc networks. A ferry-based intrusion detection and mitigation (FBIDM) scheme for sparsely connected ad hoc networks that use Prophet as their routing scheme. Via simulations, we study the effectiveness of the FBIDM scheme when malicious nodes launch selective data dropping attacks. Mutual correlation detection scheme (MUTON) for addressing these insider attacks. MUTON takes into consideration of the transitive property when calculating the packet delivery probability of each node and correlates the information collected from other nodes. Probabilistic Misbehaviour Detection Scheme for DTN, to adaptively detect misbehaviours in DTN and achieve the trade-offs between the detection cost and the detection performance. In this paper, we examine the impact of the Blackhole attack and its variations in DTN routing. We focused on the concept of encounter tickets to secure the evidence of each contact. In this scheme, nodes adopt a unique way of interpreting the contact history by making observations based on the collected encounter tickets. N disruption tolerant networks (DTNs), selfish or malicious nodes may drop received packets. Such routing misbehaviour reduces the packet delivery ratio and wastes system resources such as power and bandwidth. Although techniques have been existing to mitigate routing misbehaviour in mobile ad hoc networks, they cannot be directly applied to DTNs because of the intermittent connectivity between nodes. To address this problem, we

propose a distributed scheme to detect packet dropping in DTNs. In our existing scheme, a node is required to keep a few signed contact records of its previous contacts, based on which the next contacted node can detect if the node has dropped any packet. Since misbehaving nodes may misreport their contact records to avoid being detected, a small part of each contact record is disseminated to a certain number of witness nodes, which can collect appropriate contact records and detect the misbehaving nodes.

5. Analysis of Attack Detection Techniques

We have studied and analyse these attack detection techniques for DTN such as FBIDM, Encounter ticket based scheme, MUTON, Distributed scheme, Trust based framework, PMDS and so on. It is clear that there is a need to develop a scheme which can defend against collusion attacks. Below Table shows the work which requires further attention as well as the work which has already been attempted by different researchers in the area of Blackhole and Greyhole attack detection with collusion attack detection.

Attacks → / Techniques ↓	Individual attack	Blackhole attack	Greyhole attack	Collusion attack
FBIDM	✓	✓	?	?
Encounter ticket based scheme	✓	?	?	?
MUTON	✓	✓	?	?
Distributed scheme	✓	?	?	?
Trust based framework	✓	✓	✓	?
PMDS	✓	✓	✓	?

6. Modules

A. Network Formation and Authority Creation

First we can create a Trusted Authority and then create network node assume the communication range of a node is finite. Thus a data sender out of destination node's communication range can only transmit packetized data via a sequence of intermediate nodes in a multi-hop manner. For the simplicity of presentation, we take a three-step data forwarding process as an example. Suppose that node A has packets, which will be delivered to node C. Now, if node A meets another node B that could help to forward the packets to C, A will replicate and forward the packets to B. Thereafter, B will forward the packets to C when C arrives at the transmission range of B. In this process, we define three kinds of data forwarding evidences. They are Delegation Task Evidence, Forwarding History Evidence and Contact History Evidence, Encounter Records, Message Records.

B. Route Finding and Data Forwarding

A normal node will honestly follow, forward the messages as long as there are enough contacts. The requested message has been forwarded to the next hop, the chosen next hop nodes. We assume a trusted authority with the right to assign each node a unique identifier and a pair of public and private keys. Nodes are assumed to know the public keys of each other so that they can authenticate messages signed by others. We model the general behaviours of nodes as follows. When two nodes encounter and exchange messages, each of them generates an Encounter Record (ER) and stores it in its own storage. The ER includes the identities of two nodes, the ER sequence numbers assigned by them, the encounter timestamp and the lists of sent and received messages between the two parties and their signatures.

C. Detecting for colluding Attacks

When two nodes are communicating via intermediate node, sometimes individual's adversaries launches an attacker. First receives messages from other nodes but later drops them with a certain probability. Blackhole attacker drops all received messages (dropping probability = 100%) while grey hole attacker drops partially (dropping probability lower than 100 percent). The dropping occurs even if the attacker still has enough buffer to store messages, Introduces SDBG, which could launch the trusted authority based watchdog for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. Each node maintains a local black list which lists malicious nodes that it detects as black hole or grey hole attackers by the metrics Relaying Ratio (RR) and Self Forwarding Ratio (SFR). RR is the ratio between total number of messages that the node received and already forwarded to another node (NRS) and total number of messages received by node and not sent (NRNS). SFR is the ratio between total number of messages generated and sent (Nself-send) and total number of messages sent (Nsend).An attacker is likely to have it metrics RR and/or SFR violate the threshold.

$$RR = \frac{N_{RS}}{N_{RNS}} < Th_{RR}$$

$$SFR = \frac{N_{self\_send}}{N_{send}} > Th_{SFR}$$

ThRR is threshold RR of the node and ThSFR is threshold SFR of node. If any node is detected as committing either misbehaviours, authority will punish it accordingly and then trusted authority add blacklist and send malicious node name to all nodes. . To further improve the performance of the proposed Statistical -based Detection on scheme, we introduce a reputation system, in which the inspection probability could vary along with the target node's reputation. Under the reputation

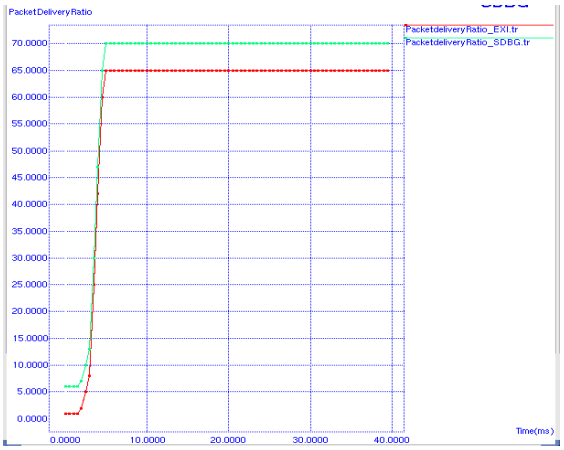
International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

system, a node with a good reputation will be checked with a lower probability while a bad reputation node could be checked with a higher probability.

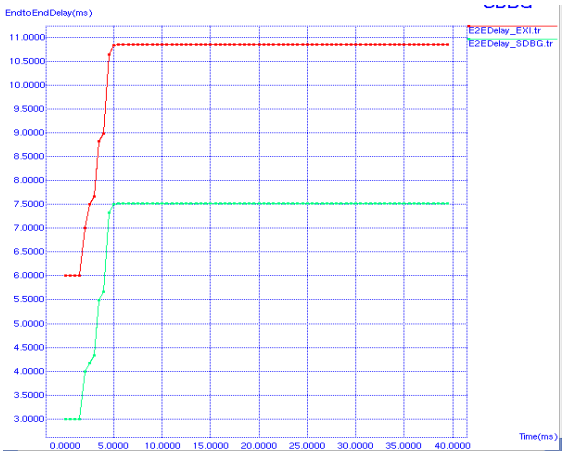
7. Results

The simulation results states that the SDBG is better than the existing scheme. These simulations mainly focused on Packet Delivery Ratio, End2End Delay, Packet Loss, Routing Overhead and Storage Overhead of the network.

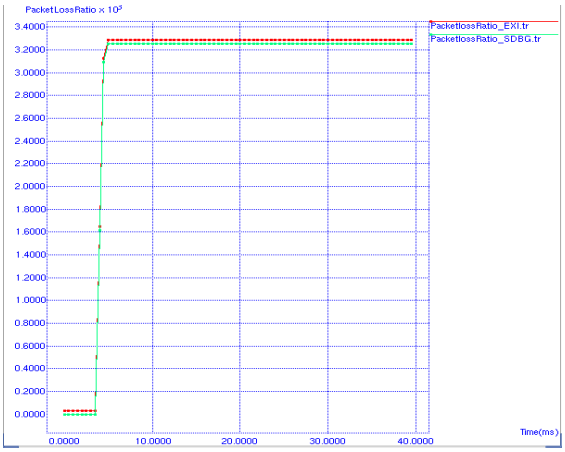
Packet Delivery Ratio-Existing vs SDBG:



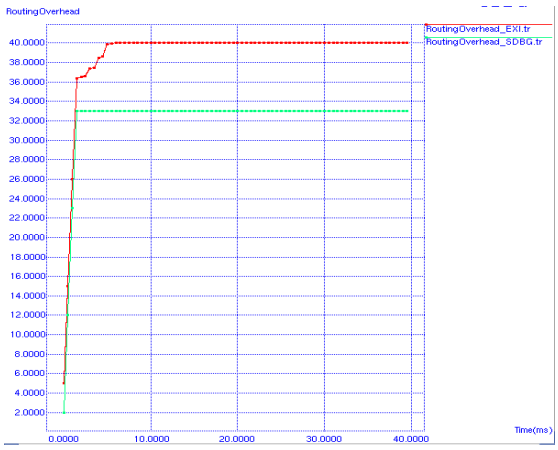
End2End Delay-Existing vs SDBG:



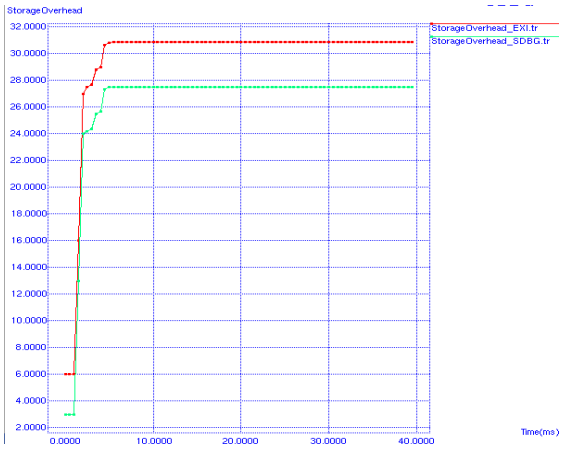
Packet Loss-Existing vs SDBG:



Routing Overhead-Existing vs SDBG:



Storage Overhead--Existing vs SDBG:



8. Conclusion

The simulation results shows that SDBG can detect colluding malicious nodes with less delay and

overhead, when varying the number of colluding nodes and with a wide range of packet dropping Probability and different routing protocols. We briefly summarize how the other two schemes work .Similar to SDBG, MDS suggests statistical metrics based on encounter history to judge nodes but it does not consider dealing with collusion attacks. We have studied various attack detection techniques in Delay Tolerant Network and compared them. From the literature reviewed, it is clear that a lot of work has been done in this area but there is a need to develop a scheme to detect collusion attacks. Various methods have been studied in literature review used for detection and prevention of Blackhole and Greyhole attackers. There may be many other methods too, by which we can prevent malicious node and increase packet delivery ratio, end to end delivery, reduce the dropping of packet and increase throughput of the system. In future we will enhance the performance and increase the packet delivery ratio more.

9. References

[1] Pham Thi Ngoc Diep,Chai Kiat Yeo,"Detecting Colluding Blackhole and Greyhole Attacks in DTN" in Mobile Computing ,pp.1536-1233,IEEE 2015

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in CRYPTO 2001, Advances in Cryptology, no. 2139 in Lecture Notes in Computer Science, pp. 213–229, Springer-Verlag, August
2001

[3] A. Lindgren, A. Doria and O. Schelen, "Probabilistic routing in intermittently connected networks," In Proc. First International Workshop on Service Assurance with Partial and Intermittent Resources (SAPIR), 2004.

[4] Q. He, D. Wu, and P. Khosla, "SORI: A secure and objective reputation based incentive scheme for ad hoc networks," in Proc. WCNC, Atlanta,GA, Mar. 2004, pp. 825–830.

[5] Y. Wang, S. Jain, M. Martonosi, and K. Fall, "Erasure coding based routing for opportunistic networks," in Proceeding of Sigcomm WDTN Workshop, August 2005.

[6] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: a secure multilayer credit based incentive scheme for delay-tolerant networks," IEEE Trans. Veh. Technol, vol. 58, no. 8, pp. 4628-4639, 2009.

[7] M. Elizabeth, Daly, and Mads Haahr, "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs" IEEE, vol.8, 2009.

[8] R. Lu, X. Lin, H. Zhu and X. Shen, " Pi: a practical incentive pro- tocol for delay tolerant networks," in IEEE Transactions on Wireless Communications,vol.9,no.4,pp.1483-1493,2010.

[9] Fani Tsapeli and Vassilis Tsaoussidis, "Routing for Opportunistic Networks Based on Probabilistic Erasure Coding," in Proc. WWIC 2012, LNCS 7277,August 2012, pp. 257–268.

[10] Shuchita Upadhyaya and Karishma, "A Co-operative Mechanism to Contrast Black-hole Attacks in Delay Tolerant Networks ", IOSR Journal of Computer Engineering (IOSR-JCE), 2016, pp. 1-5.

[11] Y. Zhang, W. Lou, W. Liu, and Y. Fang, "A secure incentive protocol for mobile ad hoc networks," Wirel. Netw., vol. 13, no. 5, pp. 569–582,Oct. 2007. Istanbul, Turkey, June 2006.

[12] M. Chuah, P. Yang, and J. Han, "A ferry-based intrusion detection scheme for sparsely connected adhoc networks," in Proceedings of first workshop on security for emerging ubiquotous computing, 2007.

[13] F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole attacks in disruption-tolerant networks using encounter tickets", in Proc. IEEE INFOCOM , pp. 2428-2436.2009

[14] Q. Li, S. Zhu, and G. Cao," Routing in Socially Selfish Delay-Tolerant Networks", Proc. IEEE INFOCOM 10, pp.1-9, 14-19, March 2010.

[15] T. Hossmann, T. Spyropoulos, and F. Legendre," Know the Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing", Proc. IEEE INFOCOM 10, 2010.

[16] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Muton: Detecting malicious nodes in disruptiontolerant networks," in WCNC 2010, pp. 1-6, 2010.

[17] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Detecting wormhole attacks in delay tolerant networks", IEEE Wireless Commun. Mag., vol. 17, no. 5, pp. 36-42, Oct. 2010.

[18] E. Ayday, H. Lee and F. Fekri "Trust Management and Adversary Detection for Delay Tolerant Networks," in Milcom'10, 2010.

[19] 2011. W. Gao and G. Cao "User-centric data dissemination in disruption tolerant networks", in Proc. of IEEE INFOCOM, 2011

[20] Lifei Wei, Haojin Zhu, Zhenfu Cao, and Xuemin (Sherman) Shen "MobiID: A User-Centric and Social-Aware Reputation Based Incentive Scheme for Delay/Disruption Tolerant Networks" H. Frey, X. Li, and S. Ruehrup (Eds.): ADHOC-NOW 2011, LNCS 6811, pp. 177–190, 2011.©Springer-Verlag Berlin Heidelberg 2011

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

[21] Q. Li and G. Cao, " Mitigating Routing Misbehavior in Disruption Tolerant Networks", IEEE Trans. Information Forensics and Security,vol.7, no. 2, pp. 664-675, Apr. 2012 .
[22] Mythili M., Renuka K. " An Efficient Black Hole and Gray Hole Detection Using Fuzzy Probabilistic Detection Scheme in DTN", International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, no. 10, pp. 123-127 , Oct. 2016.
[23] H. Zhu, S. Du, C. Xiao, R. Lu Z. Gao, "PMDS: A probabilistic misbehavior detection scheme toward efficient trust establishment in Delay-tolerant networks," IEEE Transaction on Parallel and Distributed System, vol. 25, no. 1, pp. 22-32, Jan 2014.
[24] S. K. Das N. Li, "A trust-based framework for data forwarding in opportunistic networks," Elsevier J. Ad Hoc Networking, vol. 14, pp. 1497–1509, 2013.

AUTHORS

Labala Sarathchandra Kumar
M.Tech,
Department of CS&SE,
College of Engineering,
Andhra University,
Visakhapatnam

Dr G Lavanya Devi(Ph.D)
Assistant Professor,
Department of CS&SE,
College of Engineering,
Andhra University,
Visakhapatnam.