IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

# An Efficient Black Hole and Gray Hole Detection Using Fuzzy Probabilistic Detection Scheme in DTN

**Mythili .M[1], Renuka .K M.Sc. M. Phil[2]**

Research Scholar, Department of Computer Science, Rathinam College, Coimbatore, Tamil Nadu, India [1]

Assistant Professor, Department of Computer Science, Rathinam College, Coimbatore, Tamil Nadu, India [2]

**Abstract:** Blackhole and Grayhole behaviors represent a serious threat against routing in Delay or Disruption Tolerant Networks (DTNs). Due to the unique network characteristics, designing a misbehavior detection scheme in DTN represents a great challenge. The proposed fuzzy based probabilistic attack detection scheme, for secure DTN routing. The basic idea of FPDS is introducing a periodically available vehicle to vehicle authority, which judges the node's behavior based on the collected routing evidences. The proposed model FPDS as the Inspection theoretical analysis to demonstrate that, by setting an appropriate investigation probability, the security of DTN routing at a reduced cost. To further improve the efficiency of the proposed scheme, fuzzy detection probability with a node's reputation, this allows a dynamic detection fuzzy probability determined by a node's reputation. The extensive analysis and simulation results show that the proposed scheme substantiates the effectiveness and efficiency of the proposed scheme.

**Keywords:** Delay or Disruption Tolerant Networks; Fuzzy Rule; Probability Detection; Secure Routing.

## I. INTRODUCTION

Delay Tolerant Networks have unique characteristics like lack of contemporaneous path, short range contact high variation in network conditions, difficult to predict mobility patterns and long feedback delay. Because of these unique characteristics the Delay Tolerant Networks (DTNs) move to an approach known as "store carry-and-forward" strategy where the bundles can be sent over the existing link and buffered at the next hop until next link in the path appears and the routing is determined in an "opportunistic" fashion.

The development of delay tolerant networks has bringing up a revolutionary change in the field of wireless. It is practically possible to connect the network in a region where network connectivity seems impossible. Delay tolerant networks have intermittent node connectivity and nodes in DTN are highly mobile. Due to such unusual network behavior, DTN uses store-carry-forward model as message propagation process. In store-carry-forward model, DTN node will send message to intermediate nodes only if it gets an opportunity or only if it comes in range of another node else it elects to save the node in its buffer. Also there may be possibility of long run persistent buffer storage. Sometimes, DTN nodes does not behave normally from their standard behavior and behaves abnormally intentionally tries to harm the network performance. Mostly all the networks face the problem of malicious nodes. Unlike traditional networks, it is hard to detect such type of nodes in DTN due to network inconsistency and exclusive characteristics. Malicious nodes are further divides into different categories1) selfish nodes 2) black hole nodes 3) Worm Hole 4) Sinkhole etc. This paper focused only on black hole attack. A black hole attack is an attack in which nodes silently removes or drops the entering or leaving traffic deprived of informing the source that message didn't receive destination. These nodes stay invisible in the network and are detected only when traffic lost is monitored.

DTN is threatened by various attacks, including blackhole and greyhole. Blackhole attackers drop all the received messages even if they have enough buffer storage. Greyhole attackers drop a fraction of received messages to avoid arousing suspicion and detection from other nodes. The dropping misbehavior will decrease the overall message delivery and waste the resources of intermediate nodes that have carried and forwarded the dropped messages. The lack of continuous path and limited connectivity resources in DTN make the detection of these attacks more challenging than that in a well-connected ad hoc network. Routing misbehavior detection and mitigation has been well crammed in traditional mobile ad hoc networks. These methodologies use neighbourhood monitoring or destination acknowledgement (ACK) to detect dropping of packets. In the mobile ad hoc networks (MANET) first complete route is established from source to destination, before transmitting the packet. But in DTN the nodes are intermittently connected, hence there is no possibility for route discover and it has other unique characteristics like dynamic topology, short range contact, long feedback delay which made the neighborhood monitoring unsuitable for DTN.

Most current networking protocols have been designed with the assumption that an end-to-end path between the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

packet source and the destination is almost always available. If connectivity is interrupted, then routing protocols would provide an alternative path after at most a transient outage. This is also assumed for emerging wireless Mobile Ad-hoc Networks (MANETs). However, there is an entire class of wireless networks for which this assumption does not hold. For wireless networks with intermittent connectivity, also called Delay or Disruption Tolerant Networks (DTNs), lack of continuous connectivity, network partitioning and very long delays are actually the norm, not the exception. Such networks have recently received an increasing interest due to their great potential for supporting applications deployed in challenged environments, such as vehicular networks, wireless social networks, pocket switched networks and etc.

The recent studies show that the Byzantine (insider) adversary may pose a serious threat against DTN to compromise the network performance. A Byzantine adversary (i.e., a physically captured and controlled legitimate node) can do serious damage to the network in terms of data availability, latency, and throughput. The typical examples of Byzantine attack include dropping, modifying the legitimate packets and injecting fake packets.

## II. 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 misbehavior 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 adhoc network, nodes usually have very small number of neighbours. In addition, new history based routing schemes e.g. Prophet have been proposed because traditional adhoc routing schemes do not work well in sparse ad hoc networks. In this paper, we propose 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 Misbehavior
Detection Scheme for DTN, to adaptively detect misbehaviours in DTN and achieve the tradeoffs between the detection cost and the detection performance. PMDS is motivated from the Inspection Game [8], which is a game theory model in which an inspector verifies if another party, called inspectee, adheres to certain legal rules. In this model, the inspectee has a potential interest in violating the rules while the inspector may have to perform the partial verification due to the limited verification resources. Therefore, the inspector could take advantage of partial verification and corresponding punishment to discourage the misbehaviours of inspectee. Furthermore, the inspector could check the inspectee with a higher probability than the Nash Equilibrium points to prevent the offences, as the inspectee must choose to comply the rules due to its rationality. Nodes in disruption-tolerant networks (DTNs) usually exhibit repetitive motions. Several recently proposed DTN routing algorithms have utilized the DTNs' cyclic properties for predicting future forwarding. The prediction is based on metrics abstracted from nodes' contact history. However, the robustness of the encounter prediction becomes vital for DTN routing since malicious nodes can provide forged metrics or follow sophisticated mobility patterns to attract packets and gain a significant advantage in encounter prediction. In this paper, we examine the impact of the blackhole attack and its variations in DTN routing. We introduce the concept of encounter tickets to secure the evidence of each contact. In our 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 misbehavior reduces the packet delivery ratio and wastes system resources such as power and bandwidth. Although techniques have been existing to mitigate routing misbehavior in mobile ad hoc networks, they cannot be directly applied to DTNs because of the intermittent connectivity between nodes. To address the 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.

The key requirements for security architecture in DTNs include ensuring the protection of DTN infrastructure from unauthorized use as well as application protection by

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

providing confidentiality, integrity and authentication services for end-to-end communication. In this paper, we examine the issues in providing application protection in DTNs and look at various possible mechanisms. We then existing an architecture based on Hierarchical Identity Based Encryption (HIBE) that provides end-to-end security services along with the ability to have fine-grained revocation and access control while at the same time ensuring efficient key management and distribution. We believe that a HIBE based mechanism would be much more efficient in dealing with the unique constraints of DTNs compared to standard public key mechanisms (PKI). Several application scenarios require a security design that provides fine grain access control to contents stored in storage nodes within a DTN or to contents of the messages routed through the network. The existing system proposes an access control scheme which is based on the Cipher text Policy Attributed-Based Encryption (CP-ABE) approach. One of the challenges is initial secure context establishment as it is unrealistic to assume that public key infrastructure (PKI) is always globally present and available, hence, the public key management becomes an open problem for DTN.

## III.PROPOSED APPROACH

A. Network Model

DTN mobile network scenario which involves mobile nodes communicating in ad-hoc mode with wireless technology such as Wi-fi. 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. Under the above settings, we model the general behaviors 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.

Each node i is assumed to have a unique ID Ni and a corresponding public/private key pair. We assume that each node must pay a deposit C before it joins the network, and the deposit will be paid back after the node leaves if there is no offend activity of the node. A homogeneous network with N nodes where each node communicates with a set of neighbouring nodes N (ni), which is assumed to be time-invariant for all nodes ni. We assume a broadcasting communication model where each node transmits its message to all its neighbours simultaneously. A suitable media access control (MAC) protocol is assumed to be implemented so that whenever a node broadcasts its message, it will be received by all its neighbouring nodes. We assume the deployed network is connected, i.e., there exists at least one path between any two nodes in the network.

B. Adversary Model

The proposed attack say that a node ni is misbehaving if it broadcasted its initial state falsely during time slot m = 0 or if it computed its updated function fi (·) incorrectly for at least one time slot m ≥ 0. Mathematically, node ni is misbehaving if.

$$x_{ni}(m+1) \neq f_i(X_n(n_i)(m), (x_{ni}(m)) \quad (1)$$

For at least one-time slot m ≥ 0. The set of misbehaving nodes is classified into two categories: faulty and malicious. Here assume that malicious nodes are capable of following behaviors. First, when asked by a third party verifier to give its current or previous states, a malicious node is capable of returning false states. Second, while a faulty node always broadcasts its current state truthfully to its neighbours, a malicious node is capable of broadcasting its state untruthfully. We assume, however, that malicious nodes are not colluding with each other. Specifically, each malicious node is unaware of the identity or private key of any other malicious node.

First of all, we assume that each node in the networks is rational and a rational node's goal is to maximize its own profit. In this work, we mainly consider two kinds of DTN nodes: selfish nodes and malicious nodes. Due to the selfish nature and energy consuming, selfish nodes are not willing to forward bundles for others without sufficient rewarding. As an adversary, the malicious nodes arbitrarily drop others bundles (blackhole or greyhole attack), which often take place beyond others observation, leading to serious performance degradation. Note that any of the selfish actions above can be further complicated by the collusion of two or more nodes.

C. Routing Model

The proposed routing mechanism such as First Contact routing protocol, and we assume the communication range of a mobile 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 multihop manner. Our misbehaving detection scheme can be directly used but not limited in metric-based routing algorithms, such as MaxProp and Prophet.

D. Fuzzy Rule based Detecting

The proposed system is about to design a blackhole and Grayhole attack detection system to detect the different type of attack on DTN This detection system is based on FUZZY LOGIC. We propose an IDS system in which improvement is by making use of two factors i.e. Packet Loss rate, Data Rate. We will use both factors using Fuzzy logic which is problem solving control system.

**Fuzzy Algorithm to Detect the Attack:**

1. Define a Network with N number of nodes
2. Define the Source Node S and Destination Node D
3. Set Cur Node=S as Current Node
4. While Cur Node <> DestNode a. [Repeat Steps 5 to 40]

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

5. Identify the list of neighboring nodes to Cur Node called Ne (1), Ne (2)…..Ne (M)
6. For i=1 to M
7. {
8. Identify the Analysis parameter for Each Neighbor called Packet Loss rate, Data Rate
9. [Sender End Fuzzy Logic]
10. Fuzzily these rules under the fuzzification process
11. If (Fuzzy (Packet Loss rate (Ne (i)), Low) and Fuzzy (Data Rate (Ne (i)), High)
12. {
13. Set Priority (Ne (i)) =High
14.}
15. Else If ( Fuzzy(Packet Loss rate(Ne(i)),Medium)and Fuzzy(Data Rate(Ne(i)),Medium)
16. {
17. Set Priority (Ne (i)) =Medium
18.}
19. Else If (Fuzzy (Packet Loss rate (Ne (i)), Low) and Fuzzy (Data Rate (Ne (i)), Low)
20. {
21. Set Priority (Ne (i)) =Low. (Black hole node found)
22.}
23.}
24. Find the List of High Priority Receivers from the Neighbor List called P (1), P (2)….P (K)
25. [Receiver level Fuzzy Logic]
26. For i=1 to K
27. {
28. If (Energy (P (i)) =Low)
29. {
30. Set Priority (P (i)) =Low
31.}
32. If (Data Transmitted (P (i))>THRESHOLD and Rate (P (i))>THRESHOLD)
33. {
34. Set Priority (P (i)) =priority (P (i)) +1
35.}
36.}
37.}
38. Find the Node with Max Priority called Node p
39. Set Cur Node=p
40.}

Fuzzy logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, noisy or missing information. We proposed an algorithm which is based on above factors. In this algorithm firstly we define the network with N number of nodes and we set source node to S and destination node D and after that we let current node is as source node. We repeat the steps until current node is not equal to destination node.

## IV. EXPERIMENTAL RESULTS

The simulation is implemented in java ONE simulator. The simulated network contains 40 nodes which can communicate in ad-hoc mode using Wi-Fi in a transmission range of 100 meters. They travel over an area of 4,500 m x 3,400 m, at speeds of 10-50 km/h, using Shortest Path Map Based Movement Model which is available in ONE to simulate the movement of vehicles on the streets. The simulation time is 43,200 seconds (12 hours). Messages are generated at the rate of one per 25-30 seconds. The message size is in the range of 50 kB-1 MB. This setting is applied to all the following experiments. For each experiment, the simulation runs for 10 times with random seeds and the average of the measured metrics are recorded and presented.

## V. PERFORMANCE RESULTS

The detection performance of fuzzy rule aspects: detecting probability manipulation and detecting collusion dropping. We use the following metrics for evaluation:

- Detection accuracy: percentage of malicious nodes that can be detected by normal nodes
- Detection delay: the time taken for the misbehavior to be detected.
- Detection false positive rate: percentage of normal nodes that are mistakenly judged as malicious by other normal nodes.

TABLE I DETECTION ACCURACY UNDER DIFFERENT ATTACK FOR PROPHET PROTOCOL

| Methods | Dropping Probability | | | | | |
|---|---|---|---|---|---|---|
| | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
| SDBG | 0.43 | 0.65 | 0.69 | 0.75 | 0.86 | 0.89 |
| Fuzzy Rule | 0.23 | 0.32 | 0.38 | 0.53 | 0.65 | 0.69 |

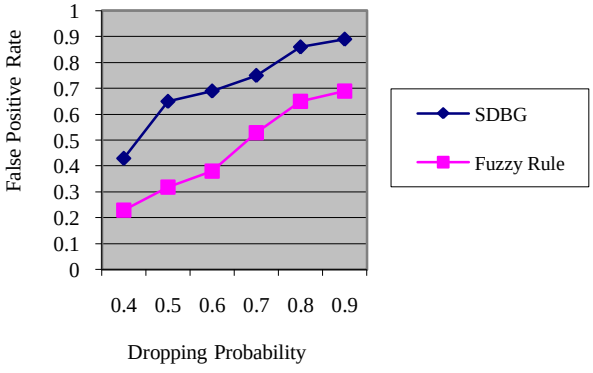


Fig. 1. False Positive Rate under Varying Attack Settings

TABLE III DETECTION TIME

| Methods | Dropping Probability | | | | | |
|---|---|---|---|---|---|---|
| | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 |
| SDBG | 564 | 675 | 764 | 854 | 934 | 1032 |
| Fuzzy Rule | 432 | 543 | 598 | 643 | 796 | 937 |

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

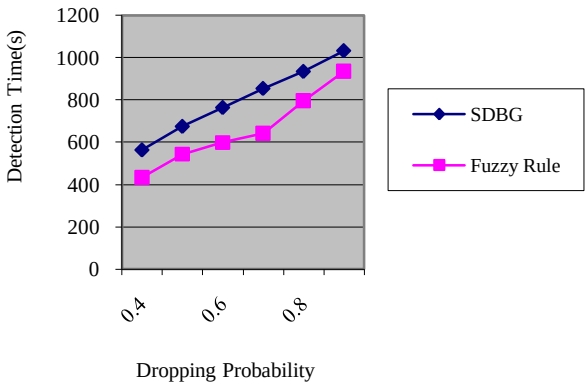


Fig. 2. Compare Detection Time under Varying Attack Settings

TABLE IIIII DETECTION ACCURACY AND FALSE POSITIVE IN PROPHET

| Methods | Fuzzy user Threshold | | | | | |
|---|---|---|---|---|---|---|
| | 3.6 | 3.8 | 4.0 | 4.2 | 4.4 | 4.6 |
| SDBG | 0.32 | 0.45 | 0.48 | 0.65 | 0.75 | 0.86 |
| Fuzzy Rule | 0.59 | 0.66 | 0.74 | 0.79 | 0.87 | 0.93 |

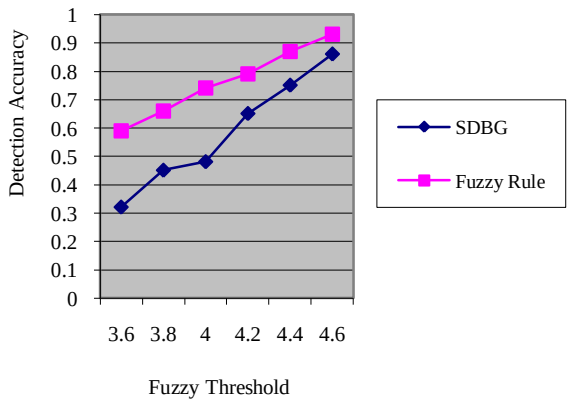


Fig. 3. Detection accuracy and false positive in Prophet under varying threshold settings

TABLE IVV DETECTION ACCURACY AND FALSE POSITIVE IN PROPHET

| Methods | Fuzzy user Threshold | | | | | |
|---|---|---|---|---|---|---|
| | 3.6 | 3.8 | 4.0 | 4.2 | 4.4 | 4.6 |
| SDBG | 2.4 | 3.5 | 5.8 | 6.4 | 8.1 | 8.9 |
| Fuzzy Rule | 1.3 | 2.7 | 3.5 | 6.4 | 7.0 | 7.2 |

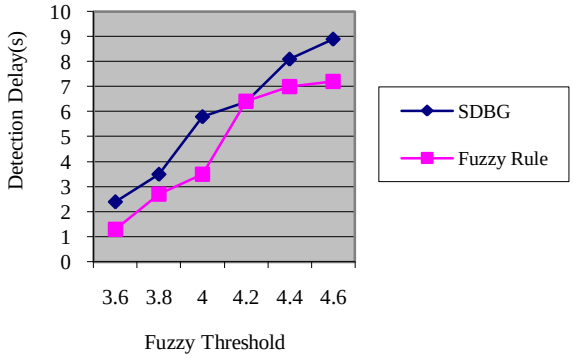


Fig 4 Detection time of Prophet under varying threshold setting

## VI. CONCLUSION

Fuzzy based Probabilistic Misbehaviour Detection Scheme (FPDS), which could reduce the detection overhead effectively. We model it as the Inspection Game and show that an appropriate probability setting could assure the security of the DTNs at a reduced detection overhead. Our simulation results confirm that FPDS will reduce transmission overhead incurred by misbehaviour detection and detect the malicious nodes effectively

## REFERENCES

[1] M. Chuah, P. Yang, and J. Han, "A ferry-based intrusion detection scheme for sparsely connected ad hoc networks," in Proc. 4th Annu. Int. Conf. Workshop Security Emerging Ubiquitous Comput. 2007, pp. 1–8.

[2] Y. Ren, M. Chuah, J. Yang, and Y. Chen, "MUTON: Detecting malicious nodes in disrupt-tolerant networks," in Proc. IEEE Wireless Common. Netw. Conf., 2010, pp. 1–6.

[3] Z. Gao, H. Zhu, S. Du, C. Xiao, and R. Lu, "PMDS: A probabilistic misbehavior detection scheme toward efficient trust establishment in Delay-tolerant networks," IEEE Trans. Parallel Distribute. Syst., vol. 25, no. 1, pp. 22–32, Jan. 2014.

[4] F. Li, J. Wu, and A. Srinivasan, "Thwarting blackhole attacks in disrupt-tolerant networks using encounter tickets," in Proc. INFOCOMM, 2009, pp. 2428–2436.

[5] Y. Guo, S. Schildt, and L. Wolf, "Detecting blackhole and greyhole attacks in vehicular delay tolerant networks," in Proc. IEEE 5th Int. Conf. Commun. Syst. Netw., Jan. 2013, pp. 1–7

[6] Q. Li and G. Cao, "Mitigating routing misbehaviours in disruption tolerant networks," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 664–675, Apr. 2012.

[7] R. Patra, S. Surana, and S. Nedevschi, "Hierarchical identity based cryptography for end-to-end security in DTNs," in Proc. Intel. Computer. Commun. Process., 2008, pp. 223–230.

[8] S. Roy, and M. Chuah, "Secure data retrieval based on cipher text policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh University, USA, 2009.

[9] Z. Jia, X. Lin, S. H. Tan, L. Li, and Y. Yang, "Public key distribution scheme for delay tolerant networks based on two-channel cryptography," J. Netw. Computer. Appl., vol. 35, no. 3, pp. 905–913, 2012.