A Secure i-Trust Scheme in Delay Tolerant Networks

[1]S.Nathiya, [2]J.Daphney Joann
[1]Student, [2]Assistant Professor
[1] Department of Computer Science and Engineering
[1]Kingston Engineering College,Vellore,India

***Abstract* - Malicious and selfish behaviors represent a serious threat against routing in delay/disruption tolerant networks (DTNs). Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. By setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost. To further improve the efficiency of the proposed scheme, correlate detection probability with a node's reputation, this allows a dynamic detection probability determined by the trust of the users. To reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively for secure DTN routing towards efficient trust establishment. Secure ZRP protocol is used to overcome the effect of the black-hole attack on the performance of the wireless networks.**

***Index Terms* - Delay tolerant networks, Misbehavior detection, Trusted Authority, Secure Zone Routing Protocol, security.**

I INTRODUCTION

In DTNs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data (e.g., sufficient buffers and meeting opportunities). Routing misbehavior can be caused by selfish (or rational) nodes that try to maximize their own benefits by enjoying the services provided by DTN while refusing to forward the bundles for others, or malicious nodes that drop packets or modifying the packets to launch attacks [1]. The recent researches show that routing misbehavior will significantly reduce the packet delivery rate thus, pose a serious threat against the network performance of DTN. Therefore, a misbehavior detection and mitigation protocol is highly desirable to assure the secure DTN routing as well as the establishment of the trust among DTN nodes in DTNs [2]. This message propagation process is usually referred to as the store-carry-and-forward strategy, and the routing is decided in an opportunistic fashion [3], [4], [5]. The security overhead incurred by forwarding history checking is critical for a DTN because expensive security operations will be translated into more energy consumptions, which represents a fundamental challenge in resource-constrained DTN. Further, even from the Trusted Authority (TA) point of view, misbehavior detection in DTNs inevitably incurs a high inspection overhead, which includes the cost of collecting the forwarding history evidence via deployed Judge nodes and transmission cost to TA.

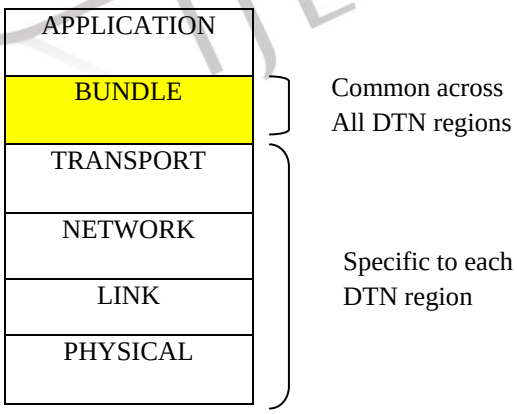

Fig 1: DTN Protocol Stack

From figure 1, Bundles consist of three things: (1) a bundle header consisting of one or more DTN blocks inserted by the bundle-protocol agent, (2) a source-application's user data, including control information provided by the source application for the destination application that describes how to process, store, dispose of, and otherwise handle the user data, and (3) an optional

bundle trailer, consisting of zero or more DTN blocks, inserted by the bundle-protocol agent. Like application-program user data, bundles can be arbitrarily long.

Therefore, an efficient and adaptive misbehavior detection and reputation management scheme is highly desirable in DTN. Mitigating routing misbehavior has been well studied in traditional mobile ad hoc networks [6]. These works use neighborhood monitoring or destination acknowledgement to detect packet dropping, and exploit credit-based and reputation-based incentive schemes to stimulate rational nodes or revocation schemes to revoke malicious nodes. Even though the existing misbehavior detection schemes work well for the traditional wireless networks, the unique network characteristics including lack of contemporaneous path, high variation in network conditions, difficult to predict mobility patterns, and long feedback delay have made the neighborhood monitoring based misbehavior detection scheme unsuitable for DTNs [4].

II SYSTEM ARCHITECTURE

A general misbehavior detection framework based on a series of newly introduced data forwarding evidences. The proposed evidence framework could not only detect various misbehaviors but also be compatible to various routing protocols [3]. Introduce a probabilistic misbehavior detection scheme by adopting the inspection game. A detailed game theoretical analysis will demonstrate that the cost of misbehavior detection could be significantly reduced without compromising the detection performance [7]. Correlate a user's reputation (or trust level) to the detection probability, which is expected to further reduce the detection probability and to demonstrate the effectiveness and the efficiency of the iTrust.

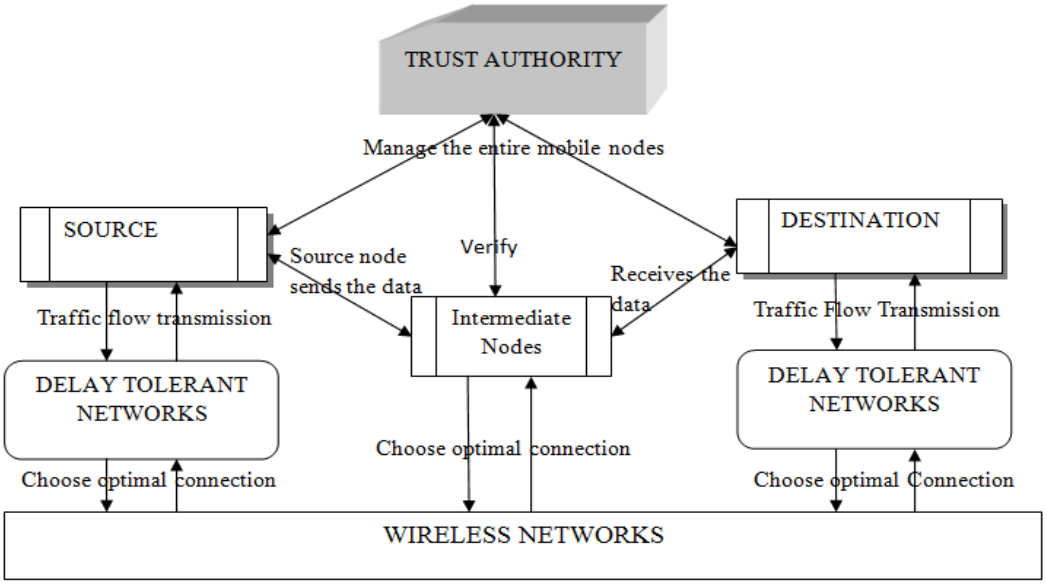

Fig 2 System Architecture: Probabilistic misbehavior detection of nodes

Figure 2 illustrates that in the routing evidence generation phase, source node forwards packets to intermediate nodes, then gets the delegation history back. Intermediate node holds the packet and then encounters destination. Destination node gets the contact history about intermediate nodes. In the auditing phase, when TA decides to check intermediate node, TA will broadcast a message to ask other nodes to submit all the evidences about intermediate node, then source node submits the delegation history from intermediate nodes, intermediate node submits the forwarding history (delegation history from destination node), destination submits the contact history about intermediate node.

III PROBABILISTIC MISBEHAVIOR DETECTION USING TRUST AUTHORITY

DTN Network Formations

A DTN consisted of mobile devices owned by individual users and each node has its unique ID and corresponding private/public key pair. By adopting the single-copy routing mechanism such as First Contact routing protocol, and assuming the communication range of a mobile node is finite [2]. 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. The basic iTrust has two phases, including routing evidence generation phase and routing evidence auditing phase.

Routing Evidence Generation Phase

Suppose, there are three nodes A, B and C. 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. There are three kinds of data forwarding evidences that could be used to judge if a node is a malicious one or not.

Delegation Task Evidence $IE_{task}^{i\to j}$

Suppose that source node N_{src} is going to send a message M to the destination N_{dst}. Without loss of generality, assume the message is stored at an intermediate node N_i, which will follow a specific routing protocol to forward M to the next hop. When N_j arrives at the transmission range of N_i, N_i will determine if N_j is the suitable next hop, which is indicated by flag bit flag. If N_j is the chosen next hop (or flag = 1), a delegation task evidence $IE_{task}^{i\to j}$ needs to be generated to demonstrate that a new task has been delegated from N_i to N_j. Given that T_{ts} and T_{Exp} refer to the time stamp and the packets expiration time of the packets, Set $IM_M^{i\to j}$ = {M, N_{src}, flag, N_i, N_j, N_{dst}, T_{ts}, T_{Exp}, Sig_{src}} where $Sig_{src} = Sig_{src}(H(M, N_{src}, N_{dst}, T_{Exp}))$ refers to the signature generated by the source nodes on message M. Node N_i generates the signature $Sig_i = SIG_i \{IM_M^{i\to j}\}$ to indicate that this forwarding task has been delegated to node N_j while node N_j generates the signature $Sig_j = SIG_j \{IM_M^{i\to j}\}$ to show that N_j has accepted this task. Therefore obtain the delegation task evidence as follows:

$$IE_{task}^{i\to j}\{ IM_{task}^{i\to j}, Sig_i, Sig_j\} \quad (1)$$

Forwarding History Evidence $IE_{forward}^{j\to k}$

When N_j meets the next intermediate node N_k, N_j will check if N_k is the desirable next intermediate node in terms of a specific routing protocol. If yes (or flag = 1), N_j will forward the packets to N_k, who will generate a forwarding history evidence to demonstrate that N_j has successfully finished the forwarding task. Suppose that

$$IM_M^{j\to k} = \{ IM_M^{i\to j}, \text{flag}, N_k, T_{ts}'\} \quad (2)$$

N_k will generate a signature $Sig_k = SIG_k \{ H(IM_M^{j\to k})\}$ to demonstrate the authenticity of forwarding history evidence. Therefore, the complete forwarding history evidence is generated by N_k as follows:

$$IE_{forward}^{j\to k} = \{IM_M^{j\to k}, Sig_k\} \quad (3)$$

which will be sent to N_j for future auditing. In the audit phase, the investigation target node will submit his forwarding history evidence to TA to demonstrate that he has tried his best to fulfill the routing tasks, which are defined by delegation task evidences.

Contact History Evidence $IE_{contact}^{j\to k}$

Whenever two nodes N_j and N_k meet, a new contact history evidence $IE_{contact}^{j\to k}$ will be generated as the evidence of the presence of N_j and N_k. Suppose that $IM^{j\to k} = \{N_j, N_k, T_{ts}\}$, where Tts is the time stamp. N_j and N_k will generate their corresponding signatures $Sig_j = SIG_j \{H(IM^{j\to k})\}$ and $Sig_k = SIG_k \{(H(IM^{j\to k})\}$. Therefore, the contact history evidence could be obtained as follows:

$$IE_{contact}^{j\to k} = \{IM^{j\to k}, Sig_k, Sig_j\} \quad (4)$$

Note that $IE_{contact}^{j\to k}$ contact will be stored at both of meeting nodes. In the audit phase, for an investigation target N_j, both of N_j and other nodes will submit their contact history evidence to TA for verification. Note that contact history could prevent the black hole or gray hole attack because the nodes with sufficient contact with other users fail to forward the data will be regarded as a malicious or selfish one.

Route Discovery and Data Forwarding

A normal user will honestly follow the first routing protocol by forwarding the messages as long as there are enough contacts. The requested message has been forwarded to the next hop, the chosen next hop nodes are desirable nodes according to a specific DTN routing protocol.

Auditing Evidence Generation Phase

In the auditing phase, TA will launch an investigation request toward node N_j in the global network during a certain period [t1, t2]. Then, given N as the set of total nodes in the network, each node in the network will submit its collected $\{IE_{task}^{i\to j}, IE_{forward}^{j\to k}, IE_{contact}^{j\to k} \mid \forall i, k \in N\}$ to TA.

By collecting all of the evidences related to N_j, TA obtains the set of messages forwarding requests $S_S$task, the set of messages forwarded $S_S$forward, and the set of contacted users $S_S$contact, all of which could be verified by checking the corresponding evidences. To check if a suspected node N_j is malicious or not, TA should check if any message forwarding request has been honestly fulfilled by N_j. Assume that $m \in S_S$task is a message sent to N_j for future forwarding and $T_{ts}(M)$ is its expiration time.

Further define $N_k(M)$ as the set of nexthop nodes chosen for message forwarding, R as the set of contacted nodes satisfying the requirements of DTN routing protocols during $[T_{ts}(M),t2]$ and D as the number of copies required by DTN routing. The misbehavior detection procedure has the following three cases:

Class I (An honest data forwarding with sufficient contacts)

A normal user will honestly follow the routing protocol by forwarding the messages as long as there are enough contacts. Therefore, given the message $m \in S_S$task, an honest data forwarding in the presence of sufficient contacts could be determined if

$m \in S_S$forward and Nk(m) $\subseteq$ R and $|N_k(m) = = D|$

which shows that the requested message has been forwarded to the next hop, the chosen next hop nodes are desirable nodes according to a specific DTN routing protocol, and the number of forwarding copies satisfy the requirement defined by a multicopy forwarding routing protocol.

Class II (An honest data forwarding with insufficient contacts)

In this class, users will also honestly perform the routing protocol but fail to achieve the desirable results due to lack of sufficient contacts. Therefore, given the message $m \in S_S$task, an honest data forwarding in the presence of sufficient contacts could be determined if

$m \notin$ Ssforward and $|R| == 0$

or

$m \in$ Ssforward and $N_k(m) == R$ and $|N_k(m)| == |R| < D$

This refers to the extreme case that there is no contact during period $[T_{ts}(m), t2]$, while shows the general case that only a limited number of contacts are available in this period and the number of contacts is less than the number of copies required by the routing protocols. In both cases, even though the DTN node honestly performs the routing protocol, it cannot fulfill the routing task due to lack of sufficient contact chances. We still regard this kind of users as honest users.

Class III (A misbehaving data forwarding with/without sufficient contacts)

A misbehaving node will drop the packets or refuse to forward the data even when there are sufficient contacts, which could be determined by examining the following rules:

$\ni m \in Ss_{task}, m \notin Ss_{forward}$ and R! 0

or

$\ni m \in Ss_{task}, m \in Ss_{forward}$ and $N_k(m) \nsubseteq R$

or

$\ni m \in Ss_{task}, m \in Ss_{forward}$ and $N_k(m) \subset R$ and $|N_k(m)| < D$

This refers to the case that the forwarder refuses to forward the data even when the forwarding opportunity is available. The second case is that the forwarder has forwarded the data but failed to follow the routing protocol. The last case is that the forwarder agrees to forward the data but fails to propagate the enough number of copies predefined by a multicopy routing protocol.

Trust Authority I-Scheme

iTrust introduces a periodically available Trust Authority (TA), which could launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes [7]. Then TA could punish or compensate the node based on its behaviors. iTrust as the Inspection Game and use game theoretical analysis to demonstrate that TA could ensure the security of DTN routing at a reduced cost via choosing an appropriate investigation probability.

Secure ZRP Protocol

The Secure Zone Routing Protocol (SZRP) is based on the concept of Zone Routing Protocol (ZRP). It is a hybrid routing protocol that combines the best features of both proactive and reactive approaches and adds its own security mechanisms to perform secure routing. The reasons for selecting ZRP as the basis of our protocol are as follows: (i) ZRP is based on the concept of routing zones, a restricted area, and it is more feasible to apply the security mechanisms within a restricted area than in a broader area that of the whole network, (ii) Since the concept of zones separate the communicating nodes in terms of interior (nodes within the zone) and exterior (nodes outside the zone) nodes, certain information like network topology and neighborhood information etc. can be hidden to the exterior nodes, (iii) Incase of a failure, it can be restricted to a zone.

However, it differs from ZRP in security aspects. In ZRP where there is no security consideration, SZRP is designed to address all measure security concerns like end to end authentication, message/packet integrity and data confidentiality during both intra and inter-zone routing. For end to end authentication and message/packet integrity RSA digital signature mechanism is employed, where as data confidentiality is ensured by an integrated approach of both symmetric and asymmetric key encryption.

IV ALGORITHM

The Basic Misbehavior Detection Algorithm

In this algorithm, Basic Misbehavior Detection, which takes j, Ss_{task} ,$Ss_{forward}$, [t1, t2],R,D as well as the routing requirements of a specific routing protocol R, D as the input, and output the detection result 1 to indicate that the target node is a misbehavior or 0 to indicate that it is an honest node. The proposed algorithm itself incurs a low checking overhead [9]. However, to prevent malicious users from providing fake delegation/forwarding/contact evidences, TA should check the authenticity of each evidence by verifying the corresponding signatures, which introduce a high transmission and signature verification overhead.

Algorithm 1. The Basic Misbehavior Detection Algorithm

1:procedure BASICDETECTION((j, Sstask, Ssforward, [t1,t2],R,D))
2: for Each m $\in$ Sstask do
3: if m $\notin$ Ssforward and R! = 0 then
4: return 1
5: else if m $\in$ Ssforward and Nκ(m) $\not\subseteq$ R then
6: return 1
7: else if m $\in$ Ssforward and Nκ(m) $\subset$ R and |Nκ(m)| < D then
8: return 1
9: end if
10: end for
11: return 0
12: end procedure

The Proposed Probabilistic Misbehavior Detection Algorithm

To reduce the high verification cost incurred by routing evidence auditing, introduce a probabilistic misbehavior detection scheme, which allows the TA to launch the misbehavior detection at a certain probability.
The advanced iTrust is motivated by the inspection game, a game theoretical model, in which an authority chooses to inspect or not, and an individual chooses to comply or not, and the unique Nash equilibrium is a mixed strategy, with positive probabilities of inspection and noncompliance [10]. For a particular node i, TA will launch an investigation at the probability of p_b. If i could pass the investigation b providing the corresponding evidences, TA will pay node i a compensation w, otherwise, i will receive a punishment C (lose its deposit).

Algorithm 2. The Proposed Probabilistic Misbehavior Detection Algorithm.

1: initialize the number of nodes n
2: for i $\rightarrow$ 1 to n do
3: generate a random number mi from 0 to 10^n - 1
4: if $m_i /10^n < p_b$ then
5: ask all the nodes (including node i) to provide evidence about node i
6: if BasicDetection (i, Sstask, Ssforward, [t1,t2],R,D) then
7: give a punishment C to node i
8: else
9: pay node i the compensation w
10: end if
11: else
12: pay node i the compensation w

13: end if
14: end for

iTrust introduces a periodically available Trust Authority (TA), which could launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes[1]. However, to prevent malicious users from providing fake delegation/ forwarding/ contact evidences, TA should check the authenticity of each evidence by verifying the corresponding signatures, which introduce a high transmission and signature verification overhead.

V The Reduction of Packet Loss Rate On iTrust

The First Contact routing protocol, which is a single-copy routing mechanism has been adopted. The packet loss rate (PLR) to indicate the misbehavior level of a malicious node. In DTNs, when a node's buffer is full, a new received bundle will be dropped by the node, and PLR denotes the rate between the dropped bundles out of the received bundles. But, a malicious node could pretend no available buffer and, thus, drop the bundles received. Figure 5.1illustrates that the PLR actually represents the misbehavior level of a node [9]. Thus, the malicious node rate has little effect on the detected rate of malicious nodes. TA could extend the inspection interval; the low inspection frequency will reduce more inspection cost because the malicious ones are all involved. But the low message generation frequency also has some advantages for TA. The misidentified rate will decrease when the message generation interval is long. Another advantage of low message generation interval is cost saved. So there is a tradeoff between the detected rate and misidentified rate when the message generation interval varies. From Figure 5.2 iTrust will improves the detection performance of TA and save the transmission cost. iTrust will be more efficient in misbehavior detection when the detection probability is small. Figure 5.3 shows the comparison of packet loss rate of the two different nodes. iTrust will reduce the authentication cost much more when the speed of nodes is very high. Figure 5.4 shows the node packet delivery measurement, the variation of the speed will not affect the effectiveness of iTrust.

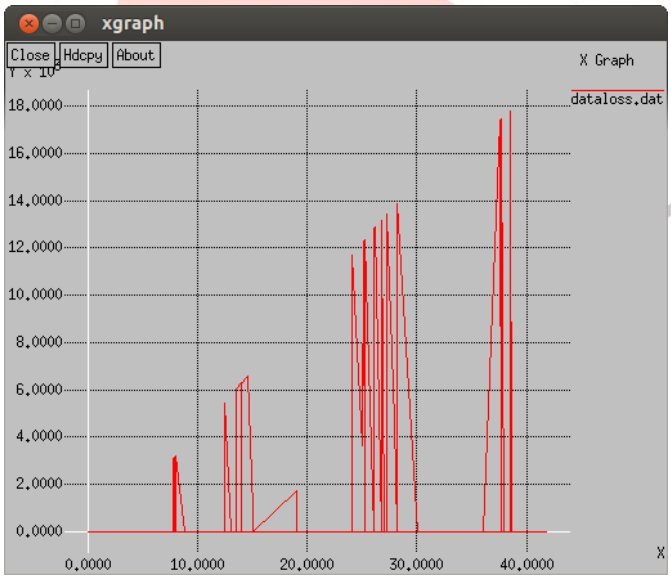

Fig 5.1 The Reduction of Packet Loss Rate using iTrust

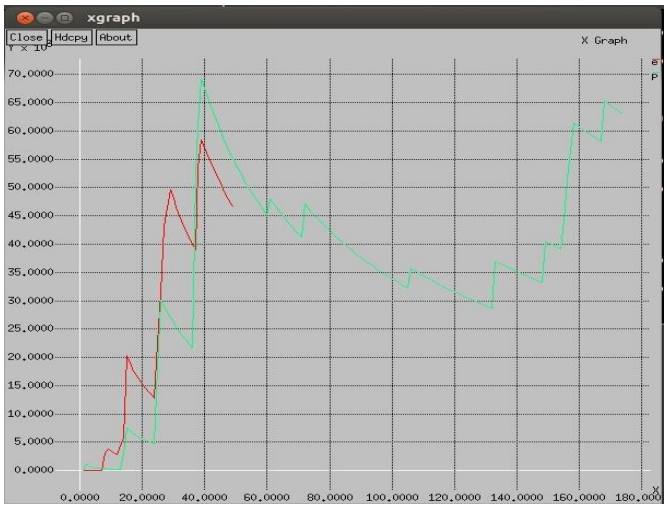

Fig 5.2 Different Detection Probabilities

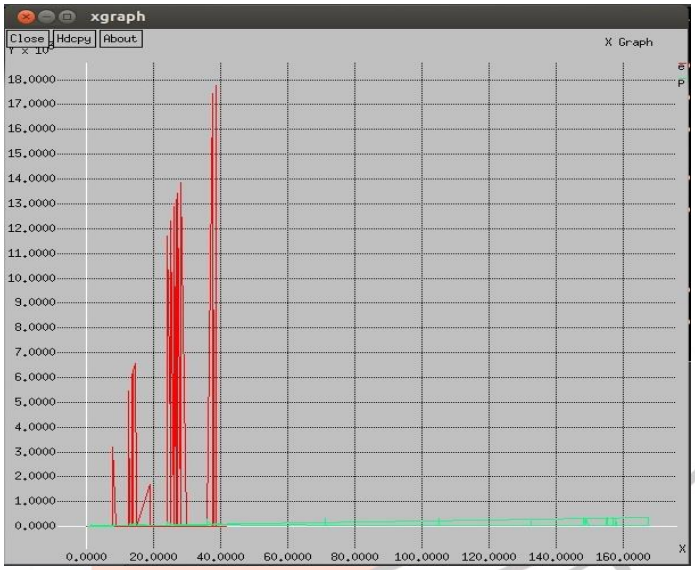

Fig 5.3 Comparison of packet loss rate with two different nodes

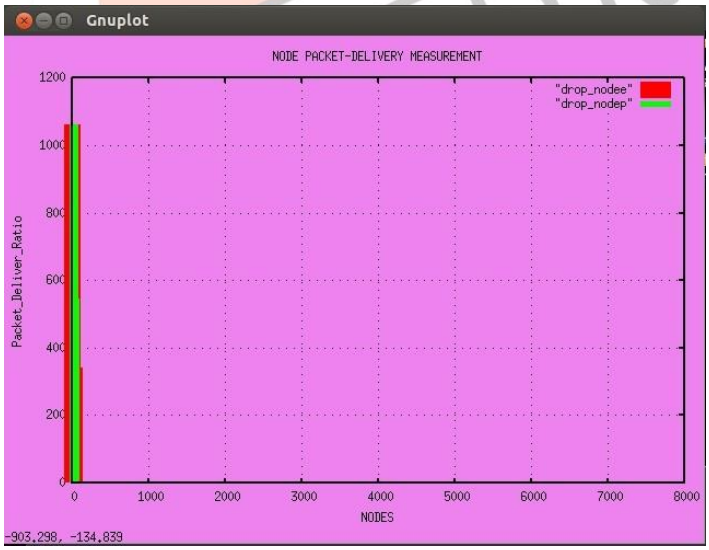

Fig 5.4 Node Packet-Delivery Measurement

VI Conclusion

The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. To reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively for secure DTN routing towards efficient trust establishment. iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing towards efficient trust establishment. TA could ensure the security of DTN routing at a reduced cost. In ZRP, there is no security consideration; SZRP is designed to address all measure security concerns like end to end authentication, message/packet integrity and data confidentiality during both intra and inter-zone routing. Therefore, efficient and adaptive misbehavior detection is highly desirable in DTN.

REFERENCES

[1] A. Lindgren and A. Doria, 'Probabilistic Routing Protocol for Intermittently Connected Networks, vol. 11, no. 9, pp. 1-11, IEEE TRANS'03, 2003.

[2] Sushant, JainKevin, FallRabin Patra, 'Routing in a Delay Tolerant Network', vol. 33, no. 2, pp. 89-112, SIGCOMM'04, 2004.

[3] Jeff Wilson 'Probabilistic Routing in Delay Tolerant Networks', vol. 8, no. 2, pp. 83-91, IEEE TRANS, 2007.

[4] Feng Li, Jie Wu,Avinash Srinivasan, 'Thwarting Blackhole Attacks in Distruption-Tolerant Networks using Encounter Tickets', vol. 7, no. 3,pp. 19-20, In Proc. of IEEE , 2008.

[5] Sushant Jain, Kevin Fall, Rabin Patra, 'Routing in Socially Selfish Delay Tolerant Networks', vol. 10, no. 4, pp. 255–268, Proc. IEEE 2009,.

[6] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xuemin (Sherman) Shen, and Bruno Preiss, 'Pi: A Practical Incentive Protocol for Delay Tolerant Networks', vol. 9, no.4, pp. 1-14, IEEE TRANS, 2010.

[7] E. Ayday, H. Lee, and F. Fekri, 'Trust Management and Adversary Detection for Delay-Tolerant Networks' Proc. Military Comm. Conf ,vol. 34, no. 3, pp. 398-406, (Milcom '10), 2010.

[8] Zhaoyu Gao*y*, Haojin Zhu*y*, Suguo Du*y*, Chengxin Xiao*y* and Rongxing Lu, 'A misbehavior detection scheme in DTN, vol. 34, no. 3, pp. 398-406, IEEE TRANS, 2011.

[9] 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, April 2012.

[10]Ameen Basha , D.S Arul Mozhi, 'Detection of misbehavior activities in delay tolerant networks', vol. 55, no. 1, pp. 117-124, IEEE TRANS 2014.