International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Misbehavior Packet Detection Approach using Effective Trust in Delay-Tolerant Networks

Prerana S. Jagadale[1], Prashant Jawalkar[2]

[1]P.G. Student, SavitribaiPhule Pune University, Department of Computer Engineering, BSIOTR, Wagholi, Pune, Maharashtra, India

[2] Assistant Professor, SavitribaiPhule Pune University, Department of Computer Engineering, BSIOTR, Wagholi, Pune, Maharashtra, India

Abstract: ***Delay Tolerant Network (DTN) have some unique network characteristics due to which finding a malicious and selfish behavior in the network is great challenge in DTN. So system with iTrust, a probabilistic misbehavior detection scheme for secure DTN routing towards efficient trust establishment is proposed here. The basic indication of iTrust is presenting a periodically existing Trusted Authority (TA) to judge the nodes behavior based on the collected routing evidences and probabilistically inspection. It also provide authentication in secure manner to all users in communication network. Proposed system will detect all the types of attack occurred in the network and detect the malicious user in network.***

Keywords: Attack,delay tolerant network, incentive scheme,iTrustmodel, misbehavior detection, security

1. Introduction

DTN, Disruption Tolerant Networking is a networking architecture that is designed to provide communications in the most unbalanced and anxious environments, where the network would usually be issue to frequent and long lasting disruptions and high bit error rates that could severely degrade normal communications.The basic thoughtbehind DTN network is that endpoints are always continuously disconnected. To facilitate data transfer, DTN uses a store-and-forward scheme across a router that is more disruption tolerant than TCP/IP. Though, the DTN approach doesn'tmean that all DTN routers on a network would require large storage capacity in order to maintain end-to-end data integrity. Disruption Tolerant Networks are often used in disaster relief missions, peace-keeping missions, and in vehicular networks.

If the nodes in a DTN are controlled by rational entities, such as people or organizations, the nodes can be behave selfishly and attempt to maximize their utilities and preserve their resources. Since routing is an inherently cooperative activity, system operation will be critically impaired unless cooperation is somehow incentivized. The need of end to end paths, high difference in network environment, and lengthy feedback delay in DTNs imply that existing solutions for mobile ad-hoc networks do not apply to DTNs.

In DTNs, a node might misbehave by dropping packets purposely still when it has the capability to forward the data. 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 packages for others, or malicious nodes that drip packets or modifying the packets to launch attacks. Themodern researches demonstrate that routing misbehavior will significantly reduce the packet delivery rate and, thus, carriage a serious threat against the network performance of DTN. Existing misbehavior detection schemes work well for the traditional wireless networks, the exclusive network features including lack of simultaneous path, high difference in network conditions, trouble to guess mobility patterns, and extended feedback delay have made the neighborhood monitoring based misbehavior detection scheme unsuitable for DTNs.

Routing misbehavior will significantly reduce the packet delivery ratio and waste the resources of the mobile nodes that have carried and forwarded the dropped packets. The security overhead incurred by the forwarding history checking is critical for a DTN because expensive security operations will be translated into extra energy consumptions, which indicates an important challenge in resource-constrained DTN. These are some drawbacks of misbehavior detection scheme and also there are some security related problems in DTN. Even from the Trusted Authority (TA) viewpoint, misbehavior detection in DTNs certainly incurs a high inspection overhead, which includes the cost of gathering the forwarding history evidence through installed judge nodes and communication cost to TA. So, awell-organized and adaptive misbehavior detection and reputation management scheme is extremelyattractive in DTN.

2. Literature Review

A. Know the Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing

Contacts seen in the history are aggregated to a social graph, and a range of metrics or algorithm have been planned to evaluate the value of a node to deliver content or bring it closer to the destination. In this paper, author argue that it is not so much the choice or complexity of social metrics and algorithms that bears the most weight on performance, but somewhat the mapping from the mobility process generating contacts to the aggregated social graph[2]. In this paper two well-known DTN routing algorithms SimBet and BubbleRap that rely on such composite network examination, and demonstrate that their performance greatly depends on how the mapping is performed.Author proposed online algorithm that uses concepts from unsupervised learning and spectral graph theory to assume this accurate graph structure, this algorithm allows each node to locally identify and correct to

Licensed Under Creative Commons Attribution CC BY

the optimal operating point, and attains goodperformance in all situations considered.

B. Routing in Socially Selfish Delay-Tolerant Networks

Existing routing algorithms for Delay Tolerant Networks (DTNs) undertake that nodes are ready to forward packets for others. But node could misbehave selfishly by ignoring or dropping packets. In this paper, author proposes a Social Selfishness Aware Routing (SSAR) algorithm [3] to allow user selfishness and offer improved routing performance in an effective way. To choice a forwarding node, SSAR studies both user's willingness to forward and their contact chance, affecting in a well forwarding system than purely contact-based methods. Trace-driven simulations show that SSAR permits users to keep selfishness and accomplishes improved routing performance with low transmission cost.

C. SMART: A SecureMultilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks

In this paper, author proposed that Delay-tolerant networks (DTNs) provide a promising solution to support wide-ranging applications in the regions where end-to-end network connectivity is unavailable. In DTNs, the intermediate nodes on a communication path are expected to store, carry, and forward the in-transit messages in an opportunistic way, which is called opportunistic data forwarding. Such a forwarding method depends on the hypothesis that each individual node is ready to forward packets for others [4]. This assumption, however, might easily be violated due to the existence of selfish or even malicious nodes, which could be unenthusiastic to waste their valuable wireless resources to function as bundle relays. To address this problem, author proposesa secure multilayer credit based incentive scheme to stimulate bundle forwarding cooperation between DTN nodes. The proposed scheme can be applied in a fully distributed manner to thwart various attacks without relying on any tamperproof hardware. In addition, we presentsome efficiency optimization techniques to improve the overall efficiency by exploiting the unique characteristics of DTNs.

D. Mitigating Routing Misbehavior in Disruption Tolerant Networks

In disruption tolerant networks (DTNs), selfish or malicious nodes could fall received packets. Such routing misbehavior decreases the packet delivery ratio and wastes system resources such as power and bandwidth. Although methods have been suggested to mitigate routing misbehavior in mobile ad hoc networks, they unsuitable to DTNs because of the intermittent connectivity between nodes. To address the problem, in this paper author proposes a distributed scheme to detect packet dropping in DTNs [8]. In this scheme, a node is required to keep a few signed contact records of its earlier contacts, based on which the next contacted node can detect if the node has released any packet. Since misbehaving nodes may misrepresent their contact records to escape being detected, a small percentage of each contact record is circulated to a certain number of witness nodes, which can gather suitable contact records and detect the misbehaving nodes. We also suggest a system to mitigate routing misbehavior by limiting the number of packets forwarded to the misbehaving nodes.

3. System Architecture

It consist of network construction, routing model, trusted model, request response based on trusted authority, data transmission.

Network Construction: In this network construction, first we have to construct a network which consists of "n" number of Nodes. Thus nodes can demand data from other nodes in the network. Subsequently the Nodes have the movement characteristics, they can move across the network. All nodes are registered in the network and each node pays some amount during the registration process. Network is used to store all the Nodes information like Node Id and other information. Also network will monitor all the Nodes Communication for security purpose. To prevent user impersonation and message modification attacks, the integrity, authenticity, and freshness of critical control messages is verified using cryptographic techniques. For example, a public key cryptosystem can be used to verify the authenticity and integrity of messages while providing confidentiality. Cryptosystems require the existence of a trusted certificate authority (CA) for initialization (issuance of keys and certificates) as well as revocation of users via a certificate revocation list (CRL).Moreover, new nodes can be added to the system after they are initialized by the CA. Every node ni is assumed to be having of a private/public key pair denoted as (ski;pki). The public key is assumed to be known to all participating nodes. This is achieved either at initialization, or via the use of certificates. In our work, we adopt a system known as ElGamal Public key encryption algorithm.

Routing Model: We adopt the singlecopy 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 nodes 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 for this system.

Licensed Under Creative Commons Attribution CC BY

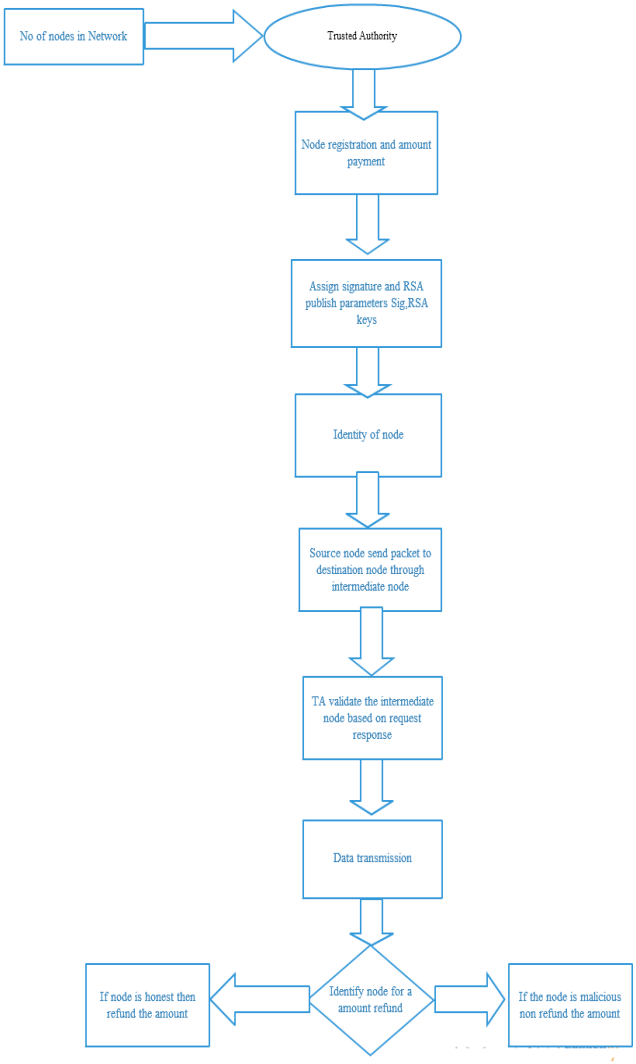


Figure 3: System architecture

Trusted Model: There are mainly two types of node are found in the network. Misbehaving node and normal node. A misbehaving node are two types firstly, selfish node that enjoy the service provide by network that refuse to carry packet for other node and malicious node that drop the received packet even if it has available buffer. But it does not drop its own packet. A normal node may drop packet when its buffer overflow, but it follows our rule. Each packet has a certain life time and then expired packet should be lost no matter there is space or not. Such dropping can be easily identified if the expiration time of packet signed by the source. Trusted authority can be distinguished between the misbehaving and normal node on the basis of its forwarding history from upstream and downstream.

Request Response based on Trusted Authority: In this module, source node in network send data to destination means, before it sends the packet to trusted authority. That packet includes source node id, intermediate node id, destination node id, packet size and time. After receiving that packet trusted authority (TA) finds which node act as intermediate node. Then it sends request to all nodes for identifying intermediate node information. Based on that request each node sends the response to TA. Although TA auditing that information for identifying intermediate node trust worthiness using basic misbehavior detection algorithm.

Data Transmission: In this module, based on TA verification each node identifies the intermediate node behavior. Then source node securely transmits the data to destination node via honest intermediate nodes. Suppose node moves one network to anothernetwork means, network verifies if the node is honest or malicious based on probabilistic misbehavior detection algorithm. Then it refunds the amount based on node gentility. If the movable node is malicious means, network didn't refund the amount.

4. The Proposed Basic iTrust Scheme In DTN

The trust has two phases that are routing evidence generation phase and auditing phase. In the routing evidence generation phase, nodes will meet another node and send the forwarding history to different nodes. In the auditing phase, trusted authority will detect whether the node is trusted or not. Suppose node A has packets which has to be delivered to node C. Now if node A meets another node B that could help to deliver packets to C, then node A will forward those packets to B. Thus, B could forward the packets to node C when C arrives at the transmission range of B. There are three steps in the routing evidence generation phase that could be used to judge if a node is a maliciousone or not.

a) Delegation task evidence
b) Forwarding history evidence
c) Contact history evidence

In the routing evidence phase, A sends packet to B, then it gets the delegation history back. B holds this packet, then faces C and C gets the contact history about B.

In the auditing phase, trusted authority will broadcast a message to ask all the other nodes to submit the evidences about B, when TA decides to check B. Then A submits the delegation history about B and C submits the contact history about B.

5. Algorithm

A. ElGamal

ElGamal Public key encryption algorithm is used for the encryption and decryption between user and the provider. The ElGamal Algorithm provides an alternative to the RSA for public key encryption. Then the basic misbehavior detection algorithm and the proposed probabilistic misbehavior detection algorithm. It consists of three phases initialization, registration, and authentication.

I. Initialization

1. Select two large prime p and q and calculate N=p*q
2. Determine key pair (e,d), ed= 1 mod Φ(N)
   a. Where , Φ(N)=(p-1)*(q-1)
3. Select generator g over fields Z*n
   a. Where, n is large odd prime number
4. Protect d, and publish (e,g,n,N).

II. Registration

1. After request of userU_i SCPC gives ID_i to user and$S_i = h(ID_i)^{2d} \ mod \ N$.

Licensed Under Creative Commons Attribution CC BY

2. As user Service provider is also register to SCPC and each Service Provider P_j with the identity ID_j maintain key pairs of signing and verifying keys.
   a. $\sigma_j(SK_j, msg)$ signing key,
   b. $Ver(PK_j, msg, \sigma_j)$ Verifying key. output is 0 or 1, signature is invalid or valid respectively.

III. Authentication

Each user has a private key x

1. User U_i send request to Service provider P_j. $msg1(req, n1)$.
2. P_j calculate its session key $Z = g^k \bmod n$
3. Set $u = Z||ID_j||\ n1$ and issue $v = \sigma_j(SK_j, u)$.
4. P_j sendmsg to U_i. $msg2(Z, v, n2)$
5. User sets $u = (Z||ID_j||n1)$ and verify $Ver(PK_j, u, v) = 0$ if output is 0 signature is invalid user terminate conversation or accept signature of P_j.
6. User select random number t and calculate w, k_{ij}, K_{ij}. Where, $w = g^t \bmod n., k_{ij} = Z^t \bmod n., K_{ij} = h(ID_j||k_{ij})$
7. For authentication user encrypt signature S_i. $P_1 = S_i \cdot y^r \bmod N$ and $P_2 = g^r \bmod N$. Where r is random integer with fixed length.
8. Then user calculate two commitment
   a. $a = (y^e)^{r1} \bmod N$
   b. $b = g^{r1} \bmod N$.
9. For NIZK proof calculates.
   a. $d_x = h(K_{ij}||w||n2||y^{er}||P_2||y^e||g||a||b)$
   b. $s = r1 - d_x \cdot r$
   Then $x = (P_1, P_2, a, b, d_x, s)$
10. User encrypt his ID_i , new nonce n3, P_j's nonce using session key K_{ij}.
    a. Cipher text $C = E_{K_{ij}}(ID_i||n2||n3)$.
11. U_i sendmsg to P_j. $msg3(w, x, C)$.
12. P_j decrypt cipher text received by user and recover $(ID_i||n2||n3)$
13. And compute $y^{er} = \frac{P_1{}^e}{h(ID_i)^2 \bmod} N$
    a. $a = (y^e)^s \cdot (y^{er})^c \bmod$
    b. $b = g^s \cdot P_2{}^c \bmod N$
14. P_j verify $(c, s) \in \{0,1\}^k \times \pm\{0,1\}^{\epsilon(l_G+k)+1}$. if output is negative terminate conversation otherwise accept msg to user with nonce $V = h(n3)$.
15. $msg4(v)$ to user.
16. User check $V = h(n3)$. true or not . if true then proceed otherwise terminate conversation.

B. The basic misbehavior detection algorithm (judge node i)

TA judges if node B is a misbehavior or not by triggering the basic misbehavior detection algorithm. In this algorithm, we introduce Find, which takes D and C as well as specific routing protocol R as the input, and output the ideal forwarding candidates W. Algorithm 1 will compare W and F. If they match, B is a good node. Else, it is malicious.

1. demand all the nodes (including node i) to provide
2. evidence D, C,F about node i
3. W=Find(Delegation Evidence D, Contact History Evidence
4. C, Routing Protocol R)
5. if F == W then
6. return 1
7. else
8. return 0
9. end if

It may cause a heavy load on TA to collect and audit various routing evidences. Due to this we will propose a basic probabilistic misbehavior detection scheme to reduce the detection overhead without compromising the system security.

C. The Proposed Probabilistic Misbehavior Detection algorithm

For a particular node i, TA will launch an investigation at the probability of pb.Ifimight pass the investigation by giving the corresponding evidences, TA will pay node i a compensation w; otherwise,i will receive a punishment P (lose its deposit).

1. initialize the number of nodes n
2. for i=1 to n do
3. generate a random number mi from 1 to (10^n - 1)
4. if mi=10n <pb then
5. ask all the nodes (including node i) to provide evidence
6. about node i
7. if Judge(node i)==1 then
8. pay node i the compensation w
9. else
10. give a punishment P to node i
11. end if
12. else
13. pay node i the compensation w
14. end if
15. end for

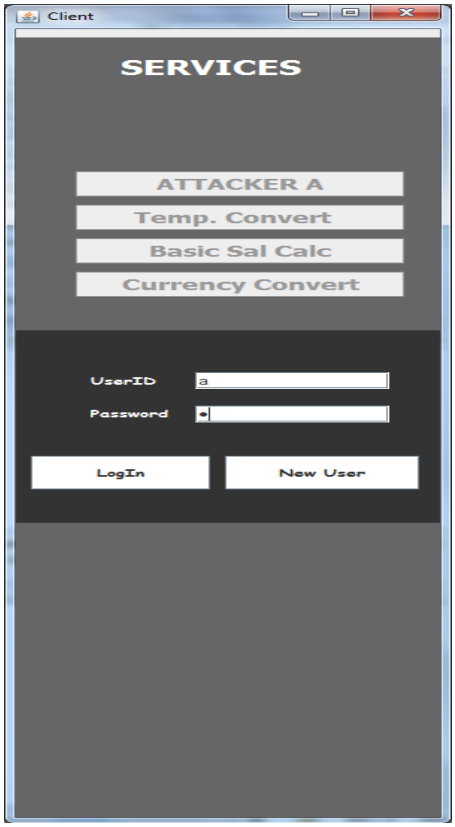
6. Results

The system is developed by using JAVA (Version JDK). The development tool used is NetBeans for desktop application. The experiments are performed on Core2Duo Intel processor 2 GB RAM. Socket programming is used for the communication between user and server. Services such as temperature conversion, gross salary calculation, currency convert and weight convert are provided to user as per the demand. This is done by calculating values at server side and provides the result to client or user. When user comes in the communication range each should first register itself to the server or SCPC. When registered user want to communicate with another node in the range or want to access service at that time communication will be done using Elgamal encryption key.

A. Result of user authentication before providing services to them

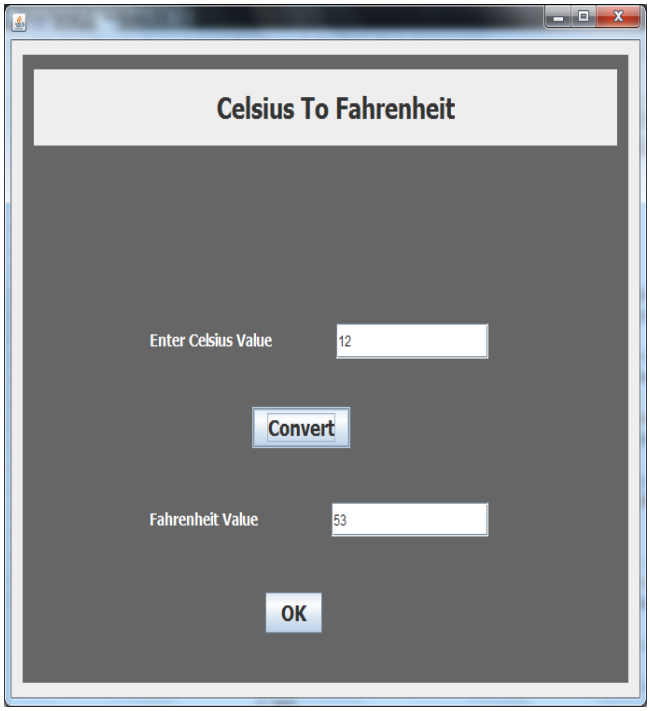
In authentication phase server will return some publish parameters. These parameters are used for transmission time authentication between different nodes.

Licensed Under Creative Commons Attribution CC BY



B. Result of temperature conversion service provided to user

Conversion of temperature from Celsius to Fahrenheit is done at server side and return to user.



C. Result of detecting malicious user

An attacker, the user having wrong signature is found as a malicious user.

7. Conclusion

Each user in the system is first authenticated before starting communication using Elgamal encryption decryption algorithm.Our system detects the different types of attack effectively at low detection overhead and provide more security to the DTN network. Due to use of effective trust scheme transmission overhead and inspection overhead is reduced.For future work we are adopting this scheme in real time system and for all the kinds of network.

8. Acknowledgement

I would like to express my sincere gratitude to my guide Prof. Prashant Jawalkarfor his continuous support, patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this paper.

References

[1] Haojin Zhu, Member, IEEE, SuguoDu, Zhaoyu Gao, Student Member, IEEE, Mianxiong Dong, Member, IEEE, and Zhenfu Cao, Senior Member, IEEE, " A Probabilistic Misbehavior Detection Scheme towardEfficient Trust Establishment in Delay-Tolerant Network ", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 1, JANUARY 2014.

[2] 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.

[3] Q. Li, S. Zhu, and G. Cao," Routing in Socially Selfish Delay-Tolerant Networks", Proc. IEEE INFOCOM 10, 2010.

[4] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks",IEEETrans. Vehicular Technology, vol. 58, no. 8, pp. 828-836, 2009.

[5] R. Lu, X. Lin, H. Zhu and X. Shen,"Pi: a practical incentive protocol for delay tolerant networks", in IEEE

Licensed Under Creative Commons Attribution CC BY

Transactions on Wireless Communications,vol.9, no.4, pp.1483-1493, 2010.
[6] F. Li, A. Srinivasan, and J. Wu," Thwarting Black hole Attacks in Disruption-Tolerant Networks Using Encounter Tickets",Proc.IEEEINFOCOM 09, 2009.
[7] A. Lindgren and A. Doria," Probabilistic Routing Protocol for Intermittently Connected Networks",draft-lindgren-dtnrg-prophet-03, 2007.
[8] 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

Licensed Under Creative Commons Attribution CC BY