© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Secure I-Trust Scheme Towards Periodic Trust Establishment in Delay-Tolerant Networks

K. Punitha, A. Pushpalatha, R. Sridurga, J. Seetha
Department of Information Technology, Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India

ABSTRACT

Malicious and selfish behaviors represent a serious threat against routing in Delay/Disruption Tolerant Networks (DTNs).We propose an iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing towards efficient trust establishment. 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. TA could ensure the security of DTN routing at a reduced cost.

Keywords: DTN, TA, Delay Tolerant Networks, WIMAX, Disruption Tolerant Networks

I. INTRODUCTION

The aim this research is to reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively for secure DTN routing towards efficient trust establishment. In existing system, the data transmissions take place in a batch model which reduces the transmission overhead. It is static and it does not find any attacks during data transmission. Here the Trusted Authority will be mostly in offline; hence TA could not detect any misbehavior activities. In some hybrid DTN network environment, the transmission between TA and each node could be also performed in a direct transmission manner (e.g., WIMAX or cellular networks). We argue that since the misbehavior detection is performed periodically, the transmission could be performed in a batch model, which could further reduce the transmission overhead. Only consider either of misbehavior detection or incentive scheme.

Proposed System

In our proposed system we have introduced a general misbehavior detection framework based on the serious of newly introduced data forwarding evidences. This framework could not only detect various misbehaviors but also be compatible to various routing protocols. Also we proposed iTrust a probabilistic misbehavior detection scheme, for secure DTN routing towards efficient trust establishment. The node's behaviors are judged by the Trusted Authority(TA) periodically. TA could ensure the security of DTN routing at a reduced cost. To improve the efficiency of this scheme, we correlated detection probability with a nodes reputation which allows dynamic detection determined by the trust of the users.

II. METHODS AND MATERIAL

A. Threat Model

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 reward. As an adversary, the malicious nodes arbitrarily drop others' bundles (black hole or gray hole attack), which often take place beyond others' observation in a sparse DTN, 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.

B. Design Requirements

The design requirements include distributed. We require that a network authority responsible for the administration of the network is only required to be periodically available and consequently incapable of monitoring the operational minutiae of the network robust. We require a misbehavior detection scheme that could tolerate various forwarding failures caused by various network environments. Scalability. We require a scheme that works independent of the size and density of the network.

The Proposed Basic iTRUST Scheme For Misbehavior Detection in DTNs

In this section, we will present a novel basic iTrust scheme for misbehavior detection scheme in DTNs. As shown in Fig. 2, the basic iTrust has two phases, including routing evidence generation phase and routing evidence auditing. In the evidence generation phase, the nodes will generate contact and data forwarding evidence for each contact or data forwarding. In the subsequent auditing phase, TA will distinguish the normal nodes from the misbehaving nodes.

3.1 Routing Evidence Generation Phase

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 that could be used to judge if a node is a malicious one or not. Delegation task evidence IEi! jtask. Suppose that source Node Nsrc is going to send a message M to the destination Ndst. Without loss of generality, we assume the message is stored at an intermediatenode Ni, which will follow a specific routing protocol to forward M to the next hop. When Nj arrives at the transmission range of Ni, Ni will determine if Njis the suitable next hop, which is indicated by flag bit flag. If Njis the chosen next hop (or flag ¼ 1), a delegation task evidence IEi!j task needs to be generated to demonstrate that a new task has been delegated from Ni to Nj. Given that Tts and TExprefer to the time stamp and the packets expiration time of the packets, we set IMi!j M ¼ fM;Nsrc; flag;Ni;Nj;Ndst; Tts; TExp; Sigsrcg, where Sigsrc¼ SigsrcðHðM;Nsrc;Ndst; TExpÞÞrefers to the signature generated by the source nodes on message M. Node Ni generates the signature Sigi¼SIGifIMi!j M gto indicate that this forwarding task has been delegated to node Njwhile node Nj generates the signature Sigj¼ SIGjfIMi!jMg to show that Njhas accepted this task. Therefore, we obtain the delegation task evidence as follows:

IEi!jtask ¼ _IMi!jM ; Sigi; Sigj_: ð1Þ

Note that delegation task evidences are used to record the number of routing tasks assigned from the upstream nodes to the target node Nj. In the audit phase, the upstream nodes will submit the delegation task evidences to TA for verification. Forwarding history evidence IEj!k forward. When Nj meets the next intermediate node Nk, Nj will check if Nk is the desirable next intermediate node in terms of a specific routing protocol. If yes (or flag ¼ 1), Nj will forward the packets to Nk, who will generate a forwarding history evidence to demonstrate that Nj has successfully finished the forwarding task.

Suppose that IMj!kM ¼ fIMi!jM ; flag;Nk; T0tsg. Nk will generate a signature Sigk ¼ SIGkfHðIMj!kMÞg to demonstrate the authenticity of forwarding history evidence. Therefore, the complete forwarding history evidence is generated by Nk as follows:

IEj!kforward ¼ _IMj!kM ; Sigk_; ð2Þ

which will be sent to Nj 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 IEj$kcontact. Whenever two nodesNj and Nk meet, a new contact history evidence IEj$k contact will be generated as the evidence of the presence of Nj and Nk. Suppose that IMj$k ¼ fNj;Nk; Ttsg, where Tts is the time stamp. Nj and Nk will generate their corresponding signaturesSigj ¼ SIGjfHðIMj$kÞg and Sigk ¼ SIGkfHðIMj$kÞg. Therefore, the contact history evidence could be obtained as follows:

IEj$kcontact ¼ _IMj$k; Sigj; Sigk_: ð3Þ

Note that IEj$kcontact will be stored at both of meeting nodes. In the audit phase, for an investigation target Nj, both of Nj 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. In the next section, we will show how to exploit three kinds of evidences to launch the misbehavior detection.

3.2 Auditing Phase

In the auditing phase, TA will launch an investigation request toward node Nj in the global network during a certain period ½t1; t2_. Then, given N as the set of total nodes in the network, each node in the network will submit its collectedfIEi!jtask; IEj!kforward; IEj$kcontact j 8i; k 2 Ng to TA. By collecting all of the evidences related to Nj, TA obtains the set of messages forwarding requests SStask, the set of messages forwarded SSforward, and the set of contacted users SScontact, all of which could be verified by checking the corresponding evidences. To check if a suspected node Nj is malicious or not, TA should check if any message forwarding request has been honestly fulfilled by Nj. We assume that m 2 SStask is a message sent to Nj for future forwarding and TtsðmÞ is its expiration time. sThe 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 2 SStask, an honest data forwarding in the presence of sufficient contacts could be determined as m 2 SSforwardand NkðmÞ _ R and jNkðmÞj ¼¼ D; ð4Þ 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 2 SStask, an honest data forwarding in the presence of sufficient contacts could be determined if m62 SSforwardand jRj ¼¼ 0 ð5Þ or m2 SSforwardand NkðmÞ ¼¼ R andjNkðmÞj ¼¼ jRj<D: ð6Þ Equation (5) refers to the extreme case that there is no contact during period ½TtsðmÞ; t2_, while (6) 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:

9m 2 SStask;m62 SSforwardand R! ¼ 0 ð7Þ Or 9m 2 SStask; m2 SSforwardand NkðmÞ 6_ R ð8Þ or 9m 2 SStask;m2 SSforwardand NkðmÞ _ R andjNkðmÞj<D: ð9Þ Note that (7) 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, which is referred to (8). 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, Which is shown in (9)? Next, we give the details of the proposed scheme as follows: In particular, TA judges if node Njis a misbehavior or not by triggering the Algorithm 1. In this algorithm, we introduce Basic Detection, which takes j; SStask; SSforward, ½t1; 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.

Algorithm **1.The Basic Misbehavior Detection algorithm.**

```
procedure BASICDETECTION
((j; SStask; SSforward; ½t1; t2_;R;D))
    for Each 2 SStaskdo
        if m 62 SSforwardand R! ¼ 0 then
            return 1
        else if m 2 SSforwardand NkðmÞ 6_ R then
            return 1
        else if m 2 SSforwardand NkðmÞ _ R and
        jNkðmÞj<D then
            return 1
        end if
    end for
    return 0
end procedure
```

The proposed algorithm itself incurs a low checking overhead. 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. We will give a detailed cost analysis in Section 4.2. In the following section, inspired by the inspection game, we will propose a probabilistic misbehavior detection scheme to reduce the detection overhead without compromising the detection performance.

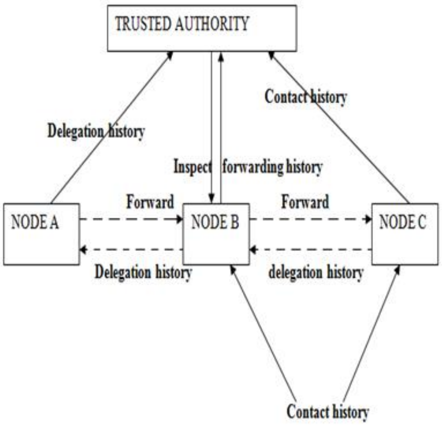

Figure 1 : Architecture diagram

III. RESULTS AND DISCUSSION

A. The Advanced iTrust: A Probabilistic Misbehavior Detection Scheme in DTNs

To reduce the high verification cost incurred by routing evidence auditing, in this section, we 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. We start from Algorithm 2, which shows the details of the proposed probabilistic misbehavior detection scheme.

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

Algorithm 2.The Proposed Probabilistic Misbehavior Detection algorithm.

```
initialize the number of nodes n
for i 1 to n do
    generate a random number mi from 0 to 10n _
    if mi=10n <pb then
        ask all the nodes (including node i) to provide evidence about node i
        if Basic Detection (i; SStask; SSforward; ½t1; t2_;R;D)then
            give a punishment C to node i
        else
            pay node i the compensation w
        end if
    else
        pay node i the compensation w
    end if
end of
```

In the next section, we will model the above described algorithm as an inspection game. And we will demonstrate that, by setting an appropriate detection probability threshold, swe could achieve a lower detection overhead and still stimulate the nodes to forward the packets for other nodes.

B. The Reduction of Misbehavior Detection Cost by Probabilistic Verification

In this section, we give a formal analysis on the misbehavior detection cost incurred by evidence transmission and verification. We model the movements and contacts as astochastic process in DTNs, and the time interval t between two successive contacts of nodes Ni and Njfollows the exponential distribution [20]: Pft_ xg ¼ 1 _ e__ijx; x 2 ½0;1Þ;

Where_ijis the contact rate between Ni and Nj, the expected contact interval between Ni and Njis E½t_ ¼ 1_ij. We further denote Costtransmissionas the evidences transmission cost and Costverificationas the evidence signature verification cost for any contact. The below Theorem 2 gives a detailed analysis on the cost incurred by iTrust.

C. Exploiting Reputation System to Further Improve the Performance of iTrust

In the previous section, we have shown that the basic iTrust could assure the security of DTN routings at the reduced detection cost. However, the basic scheme assumes the same detection probability for each node, which may not be desirable in practice. Intuitively, an honest node could be detected with a lower detection probability to further reduce the cost while a misbehaving node should be detected with a higher detection probability to prevent its future misbehavior. Therefore, in this section, we could combine iTrust with a reputation system that correlates the detection probability with nodes' reputation. The reputation system of iTrust could update node's reputation based on the previous round of detection result, and, thereafter, the reputation of this node could be used to determine its inspection probability p.We define the inspection probability p to be the inverse function of reputation. Note that p must not be higher than the bound gwþCto assure the network security level, which has been discussed before. Further, it is obvious that p cannot be larger than 1, which is the upper bound of detection probability. If a node's p is 1, it means this node has been labeled as a malicious one and, thus, should be detected for all the time. What is more important, a node with a lower reputation will lead to a higher inspection probability as well as a decrease of its expected payoff _w.

IV. CONCLUSION

In this paper, we propose a probabilistic misbehavior detection scheme (iTrust), 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 iTrust will reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively. Our future work will focus on the iTrust to other kinds of networks.

V. ACKNOWLEDGMENTS

This research was supported by National Natural Science Foundation of China (Grant No. 61003218, 70971086, 61272444, 61161140320, 61033014), Doctoral Fund of Ministry of Education of China (Grant No. 20100073120065), JSPS A3 Foresight Program, and NEC C&C Foundation. Professor Suguo Du is the corresponding author of this paper.

VI. REFERENCES

[1] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANETBased Smart Parking Scheme for Large Parking Lots," Proc. IEEE INFOCOM '09, Apr. 2009.

[2] T. Hossmann, T. Spyropoulos, and F. Legendre, "Know the Neighbor: Towards Optimal Mapping of Contacts to Social

[3] Graphs for DTN Routing," Proc. IEEE INFOCOM '10, 2010.

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

[5] 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. Vehicular Technology, vol. 58, no. 8, pp. 828-836, 2009.

[6] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks," IEEE Trans. Wireless Comm., vol. 17, no. 10, pp. 3858- 3868, Oct. 2008.

[7] 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.

[8] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom '00, 2000.

[9] R. Lu, X. Lin, H. Zhu, and X. Shen, "Pi: A Practical Incentive Protocol for Delay Tolerant Networks," IEEE Trans. Wireless Comm., vol. 9, no. 4, pp. 1483-1493, Apr. 2010.

[10] F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM '09, 2009.

[11] E. Ayday, H. Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay-Tolerant Networks," Proc. Military Comm. Conf. (Milcom '10), 2010.

[12] D. Fudenberg and J. Tirole, Game Theory. MIT Press, 1991.

[13] M. Rayay, M.H. Manshaeiy, M. Flegyhziz, and J. Hubauxy, "Revocation Games in Ephemeral Networks," Proc. 15th ACM Conf. Computer and Comm. Security (CCS '08), 2008.

[14] S. Reidt, M. Srivatsa, and S. Balfe, "The Fable of the Bees: Incentivizing Robust Revocation Decision Making in Ad Hoc Networks," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), 2009.

[15] B.B. Chen and M.C. Chan, "Mobicent: A Credit-Based Incentive System for Disruption-Tolerant Network," Proc. IEEE INFOCOM '10, 2010.

[16] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM '03, 2003.

[17] J. Douceur, "The Sybil Attack," Proc. Revised Papers from the First Int'l Workshop Peer-to-Peer Systems (IPTPS '01), 2001.

[18] R. Pradiptyo, "Does Punishment Matter? A Refinement of the Inspection Game," Rev. Law and Economics, vol. 3, no. 2, pp. 197-219, 2007.

[19] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM '06, 2006.

[20] A. Lindgren and A. Doria, "Probabilistic Routing Protocol for Intermittently Connected Networks," draft-lindgren-dtnrg-prophet-03, 20 07.

[21] W. Gao and G. Cao, "User-Centric Data Dissemination in Disruption-Tolerant Networks," Proc. IEEE INFOCOM '11, 2011.

[21] A. Keranen, J. Ott, and T. Karkkainen, "The ONE Simulator for DTN Protocol Evaluation," Proc. Second Int'l Conf. Simulation Tools and Techniques (SIMUTools '09), 2009.