Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Efficient Trust Establishment in Delay Tolerant Networks by Misbehavior Detection Scheme

D. Suguna Kuamari, Bala Veeravatnam, P. Sowmya
Department of Computer Science & Engineering in Gokaraju Rangaraju Institute of Engineering and Technology, RR Dist, Telengana, 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. In this paper, we propose iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing toward 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. We model iTrust as the inspection game and use game theoretical analysis to demonstrate that, 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, we correlate detection probability with a node's reputation, which allows a dynamic detection probability determined by the trust of the users. The extensive analysis and simulation results demonstrate the effectiveness and efficiency of the proposed scheme. Delay Tolerant Network(DTNs) are a class of unique network characterized like lack of guaranteed connectivity ,typically low frequency between DTN nodes and long propagation delay within the networks. Existing routing algorithms for DTN assumes that nodes are willing to forward packets for others but in real word selfish and malicious behaviors occurs while forward packets for nodes. Due to unique characteristics the message propagation process DTNs follows a Store-Carry and Forward manners.

Keywords: Misbehavior detection, delay tolerant networks, and Trusted authority.

I. INTRODUCTION

Delay Tolerant Networks (DTNs) have the unique feature of intermittent connectivity, which makes routing quite different from other wireless networks. Since an end-to-end connection is hard to setup, store-carry-and-forward is used to deliver the packets to the destination. In the real world, most people are selfish; we have two observations from the social perspective. First, a selfish user is usually willing to help others with whom he has social ties (e.g., friends, coworkers, roommates) will be referred to as social selfishness. Second, for those with social ties, a selfish user may give different preferences will be referred to as individual selfishness. 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. For example, the in-transit messages in DTNs, also called bundles, as shown in fig.1,could only be forwarded when two DTN nodes (N1, N2) move within each other's transmission range and contact with each other during a period of time. If no other DTN node is within the transmission range of DTN node N1, N1will buffer the current bundles and carry them until other DTN node appears within its transmission range. Therefore, the bundle propagation process in DTNs follows a "store-carry-and forward" manner and the bundles are opportunistically routed toward the destinations by intermittent connections.

Delay tolerant network providing a convenient mode of communication for civilian and business purposes, DTNs networks are highly desirable for use in battle zones, relief efforts in remote area, and difficulty situations in disaster areas. In such cases, where no network infrastructures exist, DTNs network can provide a crucial mode of communication. Delay and disruption-tolerant networks (DTNs) are characterized by their lack of connectivity, resulting in insufficiency of spontaneous end-to-end paths. A network of local networks supporting interoperability among them. An overlay on top of regional networks including the Internet accommodates long delays between and within regional networks and translates between regional network communications characteristics. The problems of DTNs can be affected by store-and-forward massage switching DTN routers need persistent storage for their queues because a communication link may not be available for a long time one node may send or receive data much faster or more reliably than the other node A message once transmitted may need to be retransmitted for some reasons. Assume communicating devices (nodes) in motion and or operation with limited power. When nodes must conserve power or preserve secrecy links are shut down intermittent connectivity network partition. On the Internet infrequent connectivity causes loss of data while DTNs disconnect delay with a store-and-forward approach. Network nodes may need to broadcast or connect during opportunistic contacts in which a sender and receiver make contact at an unscheduled time. The bundle layer a new protocol layer overlaid on top of heterogeneous region-specific lower layers with which application programs can communicate across multiple regions. Mainly nodes in DTNs are of two types which are more different from other

networks. In MANETs, routing misbehavior can severely degrade the performance at the routing layer. Specifically, nodes may participate in the route discovery and maintenance processes but refuse to forward data packets. How do we detect such misbehavior?

II. SYSTEM ANALYSIS

Problem Statement:

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 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.

Existing System:

Recently, there are quite a few proposals for misbehaviors detection in DTNs, most of which are based on forwarding history verification (e.g., multi-layered credit, three-hop feedback mechanism, or encounter ticket), which are costly in terms of transmission overhead and verification cost. The security overhead incurred by forwarding history checking is critical for a DTN since expensive security operations will be translated into more energy consumptions, which represents a fundamental challenge in resource constrained DTN.

Limitations of Existing System:

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

Proposed system:

We propose 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.

Advantages of Proposed System

- Reduce the detection overhead effectively.
- Improved Security.
- Improved Efficiency.
- Will reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively.

Trust: There are several definitions given to trust in the literature. Trust is always defined by reliability, utility, availability, quality of services and other concepts. Here, trust is defined as a belief level that one sensor node puts on another node for a specific action according to previous observation of behaviors i.e., the trust value is used to reflect whether a sensor node is willing and able to act normally in wireless sensor networks. There are three kinds of trust given as follows:

Direct Trust: Direct trust is a kind of trust which is calculated on the basis of direct communication behaviors. It reflects the trust relationship between two neighboring nodes.

Recommendation Trust: There is an efficient mechanism to filter the recommendation information. The filtered reliable recommendations are calculated as the recommendation trust.

Indirect Trust: When a subject node cannot directly observe object nodes communication behaviors, indirect trust can be established. The indirect trust value is gained based on the recommendations from other nodes. As shown in fig, 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.

Third-Party Trust:

Third-party trust refers to a situation in which two individuals implicitly trust each other even though they have not previously established a personal relationship. In this situation, two individuals implicitly trust each other because they each share a relationship with a common third party, and that third party vouches for the trustworthiness of the two people.

Certification Authority:

A Certification Authority (CA) is a trusted entity whose central responsibility is certifying the authenticity of users. In essence, the function of a CA is analogous to that of the passport issuing office in the Government. A passport is a citizen's secure document, issued by an appropriate authority, certifying that the citizen is who he claims to be (a "paper identity"). Any other country trusting the authority of that country's Government passport office will trust the citizen's passport, a good example of third-party trust.

III. IMPLEMENTAION

System Model:

We consider a normal DTN consisted of mobile devices owned by individual users. 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. We assume that a periodically available TA exists so that it could take the responsibility of misbehavior detection in DTN. For a specific detection target Ni, TA will request Ni's forwarding history in the global network. Therefore, each node will submit its collected Ni's forwarding history to TA via two possible approaches. In a pure peer-to-peer DTN, the forwarding history could be sent to some special network components via DTN transmission. In some hybrid DTN network environment, the transmission between TA and each node could be also performed in a direct transmission manner. We argue that since the misbehavior detection is performed periodically, the message transmission could be performed in a batch model, which could further reduce the transmission overhead.

Routing Model:

We adopt the single-copy 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.

Module Description:

- Information Generation Phase
- Information Investigation Phase
- Probabilistic Verification And Reputation system
- Node Clusteration

Information Generation Phase:

This phase generates information's such as the number of routing task and packet forwarding information's. This information's will be forwarded to the next phase called audit phase to detect the malicious nodes that causes threat in the network. Firstly, when a source node is about to transmit a packet to the destination node where the destination node is not in the transmission range of the source node, the source node will select an intermediate node through which it will transmit the packet the packet to the destination. The task of transmitting the packet from the source to the intermediate node and the required number of intermediate node transmission and then finally to the destination indicates the number of routing task has taken place. This is referred as the delegation task. Secondly, when a node chooses the next intermediate node and checks whether it is the desirable node to transmit the packet. If it is, then it will forward the packet. This packet forwarding information will be provided in this phase.

Information Investigation Phase:

In the audit phase the TA will verify the nodes using the information's provided from the generation phase. The generation phase will provide the routing task and the forwarding information to the authority for investigation. In order to verify the TA will initially collect the set of message forwarding requests, the set of forwarded messages and the set of contacted users.

It verifies whether the forwarding requests is satisfied and checks whether the next hop node chosen is the desirable node according to the DTN routing protocol . Further it investigates whether the multi hop forwarding is done according to the multihop routing protocol. This is how the target authority detects the malicious nodes in the network.

Probabilistic Verification and Reputation System:

In order to reduce the cost of malicious detection a probabilistic method of verification is done as explained below. This method allows the target authority to detect the malicious nodes at a certain probability. This method allows the authority to make choice to either inspect the node or not. The target authority will verify the node at a certain probability. Further it introduced a reputation system where the probability varies with the reputation of the target node. It checks the nodes reputation with the inspection probability.

Node Clusteration:

In order to increase the life time of the Delay tolerant network and to reduce the energy consumption by the nodes in the network the proposed system groups the nodes in the network into clusters. The existing work of the probabilistic method of malicious node detection will be performed in each of the clusters in the network that performs the transmission of data . This proposed work will reduce the cost which is proved in the existing system long with the

traffic reduction and time reduction in the malicious node detection in the DTN.

IV. SCREEN SHOTS

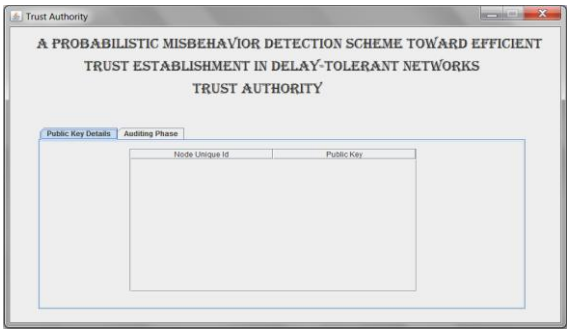

Fig: Screenshot for Trusted Authority

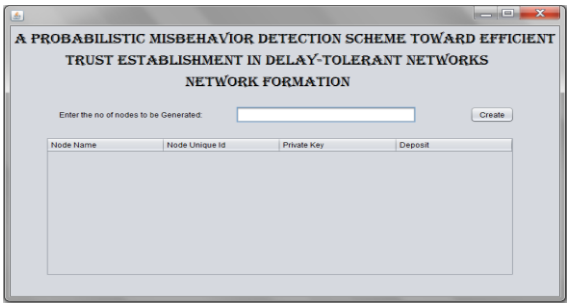

Fig: Screenshot for node generation

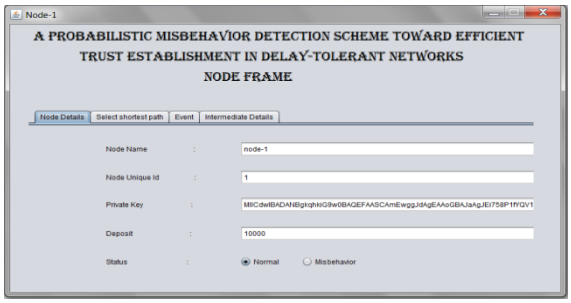

Fig: Screenshot for node details

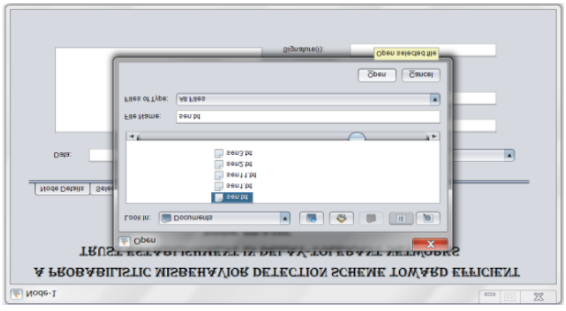

Fig : Screenshot for selecting a text file

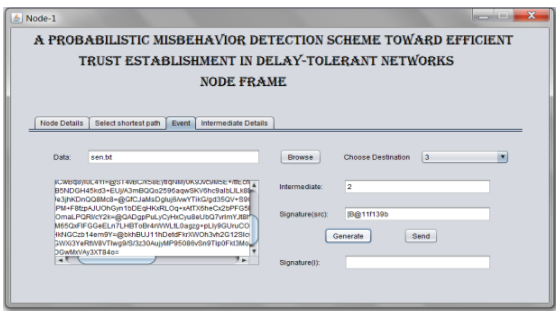

Fig: Screenshot for event select

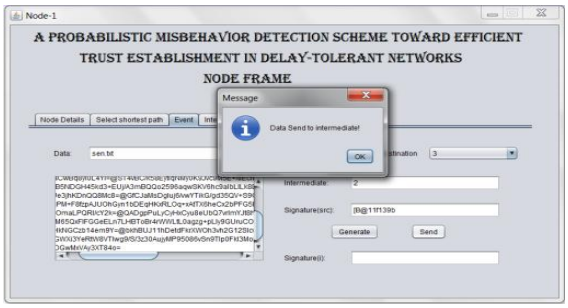

Fig: Screenshot to display a send message

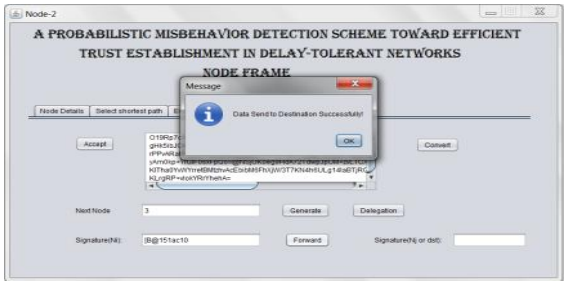

Fig: Screenshot for display destination message

V. CONCLUSION

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 extension of iTrust to other kinds of networks.

REFERENCES

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

[2] SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks Haojin Zhu, Member, IEEE, Xiaodong Lin, Member, IEEE, RongxingLu, Student Member, IEEE, Yanfei Fan, and Xuemin (Sherman) Shen, Fellow, IEEE IEEE TRANSACTIONS0ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 8, OCTOBER 2009

[3] 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.

[4] 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.

[5] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom ‟00, 2000.

[6] 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.

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

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

[9] A. Keranen, J. Ott, and T. Karkkainen, "The ONE Simulator for DTN Protocol Evaluation," Proc. SecondInt‟l Conf. Simulation Tools and Techniques (SIMUTools ‟09), 2009.

[10] A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks Haojin Zhu, Member, IEEE, Suguo Du, Zhaoyu Gao, Student Member, IEEE, Mianxiong Dong, Member, IEEE, and Zhenfu Cao, Senior Member, IEEE.

[11] http://en.wikipedia.org/wiki/Randomized_algorithm.

[12] T. Hossmann, T. Spyropoulos, and F. Legendre, "Know theNeighbor: Towards Optimal Mapping of Contacts to SocialGraphs for DTN Routing," Proc. IEEE INFOCOM '10, 2010.

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

[14] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A SecureMultilayer Credit-Based Incentive Scheme for Delay-TolerantNetworks," IEEE Trans. Vehicular Technology, vol. 58, no. 8,pp. 828-836, 2009.

[15] A. Mary Judith, V. Anusha, S. Vinod"An iTrust Based Misbehaviour Detection Technique on Clustered Nodes in Delay Tolerant Network" in IJERDT in 2014.

AUTHOR DETAILS

Mrs D.Suguna Kuamari, Post Graduated in Computer Science (M.Tech), ANU, 2010, and Graduated in Information Technology (B.Tech) From JNTU Hyderabad, 2006. She is working presently as Assitant Professor in Department of Computer Science & Engineering in Gokaraju Rangaraju Institute of Engineering and Technology, RR Dist, TS, INDIA. She has 7+ years Experience. Her Research Interests Include Networks, Software Engineering, Cloud Computing, Operating Systems and Information Security.

Mrs Bala Veeravatnam Post Graduated in Computer Science (M.Tech), JNTUH, 2012, M.C.A From JNTU Hyderabad, 2008. She is working presently as Assistant Professor in Department of Computer Science & Engineering in Gokaraju Rangaraju Institute of Engineering and Technology, RR Dist, TS, INDIA. She has 3 years Experience. Her Research Interests Include Networks, Software Engineering, Cloud Computing, Operating Systems and Information Security.

Mrs P.Sowmya, Post Graduated in Computer Science (M.Tech), JNTUH, 2014, and Graduated in Information Technology (B.Tech) From JNTU Kakinada, 2012. She is working presently as Assistant Professor in Department of Computer Science & Engineering in Gokaraju Rangaraju Institute of Engineering and Technology, RR Dist, TS, INDIA. She has 1 year Experience. Her Research Interests Include Networks, Software Engineering, Cloud Computing, Operating Systems and Information Security.

