Detection of Misbehaviour Activities in Delay Tolerant Network Using Trust Authority

J.Ameen Basha[1], D.S Arul Mozhi[2]

[1]M.E.Student, [2]Assistant professor
Department of Computer Science and Engineering,
Dhanalakshmi College of Engineering, Chennai

***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. 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. iTrust model 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, to 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 show that the proposed scheme substantiates the effectiveness and efficiency of the proposed scheme.**

Keywords - burglary; intrusion detection; fisheye lens; motion detection

I.INTRODUCTION

Delay tolerant networks (DTNs), such as sensor networks with scheduled intermittent connectivity, vehicular DTNs that disseminate location-dependent information (e.g., local ads, traffic reports, parking information), and pocket-switched networks that allow humans to communicate without network infrastructure, are highly partitioned networks that may suffer from frequent disconnectivity. In DTNs, the in-transit messages, also named bundles, can be sent over an existing link and buffered at the next hop until the next link in the path appears (e.g., a new node moves into the range or an existing one wakes up). This message propagation process is usually referred to as the "store-carry-and-forward" strategy, and the routing is decided in an "opportunistic" fashion .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. The recent researches show that routing misbehavior will significantly reduce the packet delivery rate and 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. Mitigating routing misbehavior has been well studied in traditional mobile ad hoc networks. These works use neigh- borhood 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, difficulty to predict mobility patterns, and long feedback delay, have made the neighborhood monitoring based misbehavior detection scheme unsuitable for DTNs. A launches the black hole attack by refusing to forward the packets to the next hop receiver C. Since there may be no neighboring nodes at the moment that B meets C, the misbehavior (e.g., dropping messages) cannot be detected due to lack of witness, which renders the monitoring based misbehavior detection less practical in a sparse DTN. 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 consumption- s, which represents a fundamental challenge in resource- constrained DTN. The proposed iTrust scheme is inspired from the Inspection Game, 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 ad- vantage of partial verification and corresponding punishment to discourage the misbehaviors of inspectees. 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. Inspired by Inspection Game, to achieve the tradeoff be- tween the security and detection cost, 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. Then TA could punish or compensate the node based on its behaviors.

To further improve the performance of the proposed probabilistic inspection scheme, introduced a reputation system, in which the inspection probability could vary along with the target node's reputation. Under the reputation system, a node with a good reputation will be checked with a lower probability while a bad reputation node could be checked with a higher probability. iTrust as the model for 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.

The contributions of this paper can be summarized as follows.

1. Firstly, proposed 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.
2. Secondly, introduced 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. Also discuss how to correlate a user's reputation (or trust level) to the detection probability, which is expected to further reduce the detection probability.
3. Thirdly, used extensive simulations as well as detailed analysis to demonstrate the effectiveness and the efficiency of the iTrust.

II.RELATED WORK

R. Lu, X. Lin, H. Zhu, and X. Shen says that Searching for a vacant parking space in a congested area or a large parking lot and preventing auto theft are major concerns to our daily lives. So propose a new smart parking scheme for large parking lots through vehicular communication. The proposed scheme can provide the drivers with real-time parking navigation service, intelligent anti-theft protection, and friendly parking information dissemination. Performance analysis via extensive simulations demonstrates its efficiency and practicality.[1]

Theus Hossmann, Thrasyvoulos Spyropoulos, and Franck Legendre conveys Delay Tolerant Networks (DTN) are networks of self-organizing wireless nodes, where end-to-end connectivity is intermittent. In these networks, forwarding decisions are generally made using locally collected knowledge about node behavior (e.g., past contacts between nodes) to predict future contact opportunities. The use of complex network analysis has been recently suggested to perform this prediction task and improve the performance of DTN routing. Contacts seen in the past are aggregated to a social graph, and a variety of metrics (e.g., centrality and similarity) or algorithms (e.g., community detection) have been proposed to assess the utility of a node to deliver a content or bring it closer to the destination. Here argue that it is not so much the choice or sophistication of social metrics and algorithms that bears the most weight on performance, but rather the mapping from the mobility process generating contacts to the aggregated social graph.

Well, first study two well-known DTN routing algorithms – SimBet and BubbleRap – that rely on such complex network analysis, and show that their performance heavily depends on how the mapping (contact aggregation) is performed. What is more, for a range of synthetic mobility models and real traces, To show that improved performances (up to a factor of 4 in terms of delivery ratio) are consistently achieved for a relatively narrow range of aggregation levels only, where the aggregated graph most closely reflects the underlying mobility structure. To this end, proposed an online algorithm that uses concepts from unsupervised learning and spectral graph theory to infer this "correct" graph structure; this algorithm allows each node to locally identify and adjust to the optimal operating point, and achieves good performance in all scenarios considered.[2]

E. Ayday, H. Lee and F. Fekri says that Delay Tolerant Networks (DTNs) have been identified as one of the key areas in the field of wireless communications. They are characterized by large end-to-end communication latency and the lack of end-to-end path from a source to its destination. These characteristics pose several challenges to the security of DTNs. Especially, Byzantine attacks give serious damages to the network in terms of latency and data availability. Using reputation-based trust management systems is shown to be an effective way to handle the adversarial behavior in Mobile Ad-Hoc Networks (MANETs). However, because of the unique characteristics of DTNs, the techniques to build a trust mechanism for MANETs do not apply to DTNs. The main objective is to develop a robust trust mechanism and an efficient and low cost malicious node detection technique for DTNs.

Inspired by the recent results on reputation management for online systems and e-commerce, developed an iterative malicious node detection mechanism for DTNs which is far more effective than existing techniques. The results indicate the proposed scheme provides high data availability and packet-delivery ratio with low latency in DTNs under adversary attacks[3].

Rongxing Lu, Student Member, IEEE, Xiaodong Lin, Member, IEEE, Haojin Zhu,, Xuemin (Sherman) Shen, Bruno Preis says that Delay Tolerant Networks (DTNs) are a class of networks characterized by lack of guaranteed connectivity, typically low frequency of encounters between DTN nodes and long propagation delays within the network. As a result, the message propagation process in DTNs follows a store-carry- and-forward manner, and the in-transit bundle messages can be opportunistically routed towards the destinations through intermittent connections under the hypothesis that each individual DTN node is willing to help with forwarding. Unfortunately, there may exist some selfish nodes, especially in a cooperative network like DTN, and the presence of sel fish DTN nodes could cause catastrophic damage to any well designed opportunistic routing scheme and jeopardize the whole network.,

Here to address the selfishness problem in DTNs, propose a practical incentive protocol, called Pi, such that when a source node sends a bundle message, it also attaches some incentive on the bundle, which is not only attractive but also fair to all participating DTN nodes. With the fair incentive, the selfish DTN nodes could be stimulated to help with forwarding bundles to achieve better packet delivery performance. In addition, the proposed Pi protocol can also thwart various attacks, which could be launched by selfish DTN nodes, such as free ride attack, layer removing and adding attacks. Extensive simulation results demonstrate the effectiveness of the proposed Pi protocol in terms of high delivery ratio and lower average delay [4].

F. Li, A. Srinivasan and J. Wu says that 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.

Here it examine the impact of the black hole attack and its variations in DTN routing. And introduce the concept of encounter tickets to secure the evidence of each contact. The scheme is, nodes adopt a unique way of interpreting the contact history by making observations based on the collected encounter tickets. Then, following the Dempster-Shafer theory, nodes form trust and confidence opinions towards the competency of each encountered forwarding node [5].

S. Zhong, J. Chen, Y. R. Yang says that Sprite Mobile ad hoc networking has been an active research area for several years. How to stimulate cooperation among selfish mobile nodes, however, is not well addressed yet. Well so propose Sprite, a simple, cheat-proof, credit-based system for stimulating cooperation among selfish nodes in mobile ad hoc networks. The system provides incentive for mobile nodes to cooperate and report actions honestly. Compared with previous approaches, the system does not require any tamper-proof hardware at any node. Furthermore, present a formal model of our system and prove its properties. Evaluations of a prototype implementation show that the overhead of our system is small. Simulations and analysis show that mobile nodes can cooperate and forward each other's messages, unless the resource of each node is extremely low [6].

J. Douceur says that Security is important for many sensor network applications. A particularly harmful attack against sensor and ad hoc networks is known as the Sybil attack based on J.R. Douceur (2002), where a node illegitimately claims multiple identities. Systematically analyzes the threat posed by the Sybil attack to wireless sensor networks. Demonstrate that the attack can be exceedingly detrimental to many important functions of the sensor network such as routing, resource allocation, misbehavior detection, etc. Establish a classification of different types of the Sybil attack, which enables us to better understand the threats posed by each type, and better design countermeasures against each type. Then propose several novel techniques to defend against the Sybil attack, and analyze their effectiveness quantitatively [7] .

W. Gao and G. Cao says that data dissemination is useful for many applications of Disruption Tolerant Networks (DTNs). Current data dissemination schemes are generally network-centric ignoring user interests. For this propose a novel approach for user-centric data dissemination in DTNs, which considers satisfying user interests and maximizes the cost-effectiveness of data dissemination. The approach is based on a social centrality metric, which considers the social contact patterns and interests of mobile users simultaneously, and thus ensures effective relay selection.By formal analysis, it show the lower bound on the cost effectiveness of data dissemination, and analytically investigate the tradeoff between the effectiveness of relay selection and the overhead of maintaining network information [8].

III.PROPOSED METHODOLOGY

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). 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. Only consider either of misbehavior detection or incentive scheme

Firstly, introduced data forwarding evidences for a general misbehavior detection framework based on a series. The proposed evidence framework could not only detect various misbehaviors but also be compatible to various routing protocols.Secondly, introduced 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 performance. Also discussed how to correlate a user's reputation (or trust level) to the detection probability, which is expected to further reduce the detection probability. Thirdly, use extensive simulations as well as detailed analysis to demonstrate the effectiveness and the efficiency of the iTrust.For data Security, used the RSA algorithm and Hash function for User Authentication.

A. DTN Network Formation

Adopt the single-copy routing mechanism such as First Contact routing protocol, and 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 multi-hop manner. For the simplicity of presentation, 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.

B. 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, and the number of forwarding copies satisfy the requirement defined by a multi-copy forwarding routing protocol

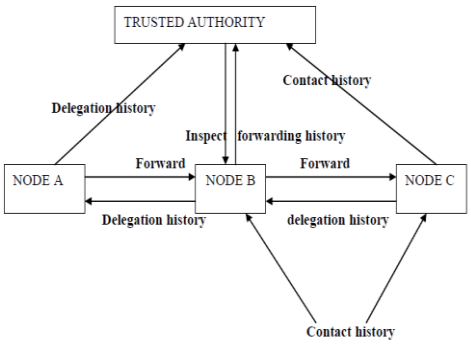


Fig 1 Syste Architecture

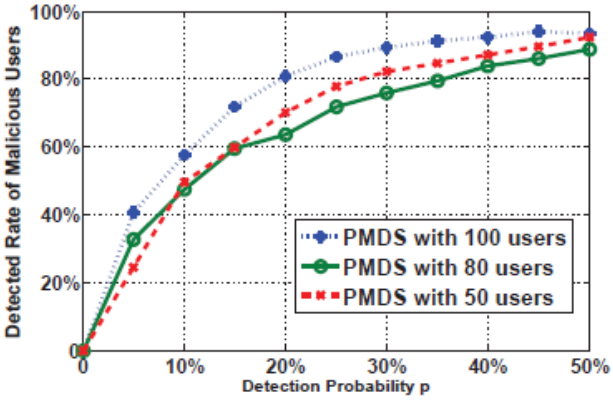
C. Trust Authority I-Scheme

The tradeoff between the security and detection cost, 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.

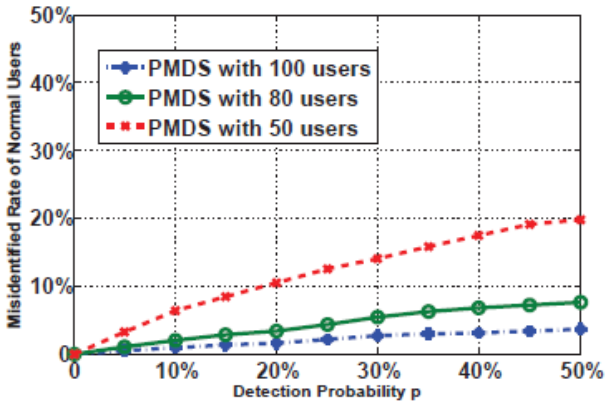
Then TA could punish or compensate the node based on its behaviors. To further improve the performance of the proposed probabilistic inspection scheme, introduce a reputation system, in which the inspection probability could vary along with the target node's reputation.

Under the reputation system, a node with a good reputation will be checked with a lower probability while a bad reputation node could be checked with a higher probability. iTrust as the model fot 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.

IV. Quality Of Service



(a) Detected rate of malicious nodes



(b) false rate of misidentified nodes

Fig 2

V. Conclusion and Future Work

A Probabilistic Misbehaviour Detection Scheme (iTrust), which could reduce the detection overhead effectively. The model has the Inspection Game and show that an appropriate probability setting could assure the security of the DTNs at a reduced detection overhead. The simulation results confirm that iTrust will reduce transmission overhead incurred by misbehaviour

detection and detect the malicious nodes effectively and the future Enhancement will focus on the extension of iTrust to other kinds of networks and reduces the bandwidth of the Trusted Authority by time variant monitoring of the nodes for malicious detection

REFERENCES

[1] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET-based Smart Parking Scheme for Large Parking Lots", in Proc. of IEEE INFOCOM'09, Rio de Janeiro, Brazil, April 19-25, 2009.

[2] T. Hossmann, T. Spyropoulos, and F. Legendre, "Know The Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing", in Proc. of IEEE INFOCOM'10, 2010.

[3] E. Ayday, H. Lee and F. Fekri"Trust Management and Adversary Detection for Delay Tolerant Networks," in Milcom'10, 2010.

[4] R. Lu, X. Lin, H. Zhu and X. Shen,Pi: a practical incentive pro- tocol for delay tolerant networks," in IEEE Transactions on Wireless Communications,vol.9,no.4,pp.1483-1493,2010.

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

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

[7] J. Douceur,"The sybil attack" in IPTPS,2002.

[8] W. Gao and G. Cao "User-centric data dissemination in disruption tolerant networks", in Proc. of IEEE INFOCOM, 2011

[9] Q. Li and G. Cao,"Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, April 2012

[10] Q. Li, S. Zhu, G. Cao, "Routing in Socially Selfish Delay Tolerant Networks" in Proc. of *IEEE Infocom'10*, 2010.