An Efficient Provest based Trust Model for Delay Tolerant Networks

Dr. P. Saveetha
(ASP/IT)
Department of Information Technology
Nandha College of Technology Erode, India

S. Anisha, V. T. Meena, S. Pradeep, S. Prem
(UG Scholar)
Department of Information Technology
Nandha College of Technology Erode, India

Abstract: **Delay tolerant networks (DTNs) are typically encountered in military network environments wherever end-to-end property isn't secure because of frequent disconnection or delay. This work prefer a provenance-based trust model, specifically PROVEST (PROVENANCE primarily based Trust model) that aims to attain correct end to end trust assessment and maximize the delivery of correct messages received by destination nodes whereas minimizing message delay and communication value underneath resource-constrained network environments. Provenance refers to the history of possession of a valued object or data. PROVEST use a data-driven approach to scale back resource utilization within the presence of egocentric or malicious nodes where as estimating a node's trust dynamically in response to changes within the environmental and node conditions.**

Keywords: Delay tolerant networks, provenance, store-and-forward, trust, trustworthiness

I. INTRODUCTION

Delay or disruption tolerant networks (DTNs) are often observed in emerging applications such as emergency response, special operations, smart environments, habitat monitoring, and vehicular ad-hoc networks where multiple nodes participate in group communications to achieve a common mission. The core characteristic of DTNs is that there is no guarantee of end-to-end connectivity, thus causing high delay or disruption due to inherent characteristics or intentionally misbehaving nodes. Managing trust efficiently and effectively is critical to facilitating cooperation or collaboration and decision making tasks in DTNs while meeting system goals such as reliability, availability, quality of service (QoS), and/or scalability. Accurate trust evaluation is especially challenging in DTN environments because nodes are sparsely scattered and do not often encounter each other. Therefore, encounter based evidence exchange among nodes may not be always possible. The lack of direct interaction experience in DTN environments hinders continuous evidence collection and can result in incorrect trust estimation, leading to poor application performance. A major challenge of a provenance-based system is that it must defend against attackers who may modify or drop messages including provenance information or disseminate fake information. Delay-tolerant networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space. Recently, the term disruption-tolerant networking has gained currency in the United States due to support from DARPA, which has funded many DTN projects. Disruption may occur because of the limits of wireless radio range, sparsity of mobile nodes, energy resources, attack, and noise. The ability to transport, or route, data from a source to a destination is a fundamental ability all communication networks must have. Delay and disruption-tolerant networks (DTNs), are characterized by their lack of connectivity, resulting in a lack of instantaneous end-to-end paths. In these challenging environments, popular ad hoc routing protocols such as AODV and DSR fail to establish routes. This is due to these protocols trying to first establish a complete route and then, after the route has been established, forward the actual data.

However, when instantaneous end-to-end paths are difficult
or impossible to establish, routing protocols must take to a "store and forward" approach, where data is incrementally moved and stored throughout the network in hopes that it will eventually reach its destination. A common technique used to maximize the probability of a message being successfully transferred is to replicate many copies of the message in the hope that one will succeed in reaching its destination. This is feasible only on networks with large amounts of local storage and inter node bandwidth relative to the expected traffic. In many common problem spaces, this inefficiency is outweighed by the increased efficiency and shortened delivery times made possible by taking maximum advantage of available unscheduled forwarding opportunities. In others, where available storage and inter node throughput opportunities are more tightly constrained, a more discriminate algorithm is required.

II. LITERATURE SURVEY

(i) Routing for disruption tolerant networks: taxonomy and design

T. Spyropoulos, R. Rais, T. Turletti, K. Obraczka, and A. Vasilakos, Wireless Networks, vol. 16, no. 8, pp. 2349–2370,2010

Communication networks, whether they are wired or wireless, have traditionally been assumed to be connected at least most of the time. However, emerging

applications such as emergency response, special operations, smart environments, VANETs, etc. coupled with node heterogeneity and volatile links (e.g. due to wireless propagation phenomena and node mobility) will likely change the typical conditions under which networks operate. In fact, in such scenarios, networks may be mostly disconnected, i.e., most of the time, end-to-end paths connecting every node pair do not exist. To cope with frequent, long-lived disconnections, opportunistic routing techniques have been proposed in which, at every hop, a node decides whether it should forward or store-and-carry a message. Despite a growing number of such proposals, there still exists little consensus on the most suitable routing algorithm(s) in this context. One of the reasons is the large diversity of emerging wireless applications and networks exhibiting such "episodic" connectivity. These networks often have very different characteristics and requirements, making it very difficult, if not impossible, to design a routing solution that fits all.

(ii) Trust management for encounter-based routing in delay tolerant networks
I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, IEEE, Global TelecommunicationsConference, Miami, FL, 6-10 Dec. 2010,pp.1–6.

We propose and analyze a class of trust management protocols for encounter-based routing in delay tolerant networks (DTNs). The underlying idea is to incorporate trust evaluation in the routing protocol, considering not only quality-of-service (QoS) trust properties (connectivity) but also social trust properties (honesty and unselfishness) to evaluate other nodes encountered. Two versions of trust management protocols are considered: an equal-weight QoS and social trust management protocol (called trust-based routing) and a QoS only trust management protocol (called connectivity-based routing). By utilizing a stochastic Petri net model describing a DTN behavior, we analyze the performance characteristics of these two routing protocols in terms of message delivery ratio, latency, and message overhead. We also perform a comparative performance analysis with epidemic routing for DTN consisting of heterogeneous mobile nodes with vastly different social and networking behaviors. properties (connectivity) but also social trust properties (honesty and unselfishness) to evaluate other nodes encountered. Two versions of trust management protocols are considered: an equal-weight QoS and social trust management protocol (called trust-based routing) and a QoS only trust management protocol (called connectivity-based routing). By utilizing a stochastic Petri net model describing a DTN behavior, we analyze the performance characteristics of these two routing protocols in terms of message delivery ratio, latency, and message overhead. We also perform a comparative performance analysis with epidemic routing for a DTN consisting of heterogeneous mobile nodes with vastly different social and networking behaviors.

(iii) Secure and reliable routing protocols for heterogeneous multihop wireless networks

M. Mahmoud, X. Lin, and X. Shen, IEEE, Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 1140–1153, March 2015.

E-STAR for establishing stable and reliable routes in heterogeneous multihop wireless networks. E-STAR combines payment and trust systems with a trust-based and energy-aware routing protocol. The payment system rewards the nodes that relay others' packets and charges those that send packets. The trust system evaluates the nodes' competence and reliability in relaying packets in terms of multi-dimensional trust values. The trust values are attached to the nodes' public-key certificates to be used in making routing decisions. We develop two routing protocols to direct traffic through those highly-trusted nodes having sufficient energy to minimize the probability of breaking the route. By this way, E-STAR can stimulate the nodes not only to relay packets, but also to maintain route stability and report correct battery energy capability. This is because any loss of trust will result in loss of future earnings. Moreover, for the efficient implementation of the trust system, the trust values are computed by processing the payment receipts. Analytical results demonstrate that E-STAR can secure the payment and trust calculation without false accusations. Simulation results demonstrate that our routing protocols can improve the packet delivery ratio and route stability.

(iv) A provenance-aware virtual sensor system using the open provenance model

Y. Liu, J. Futrelle, J. Myers, A. Rodriguez, and R. Kooper, in International Symposium on Collaborative

Sensor web applications such as real-time environmental decision support systems require the use of sensors from multiple heterogeneous sources for purposes beyond the scope of the original sensor design and deployment. In such cyber environments, provenance plays a critical role as it enables users to understand, verify, reproduce, and ascertain the quality of derived data products. Such capabilities are yet to be developed in many sensor web enablement (SWE) applications. This paper develops a provenance-aware "Virtual Sensor" system, where a new persistent live "virtual" sensor is re-published in realtime after some model-based computational transformations of the raw sensor data streams. We describe the underlying OPM (Open Provenance Model) API's (Application Programming Interfaces), architecture for provenance capture, creation of the provenance graph and publishing of the provenance-aware virtual sensor where the new virtual sensor time-series data is augmented with OPM- compliant provenance information. A case study on creating real-time provenance-aware virtual rainfall sensors is illustrated. Such a provenance-aware virtual sensor system allows digital preservation and verification of the new virtual sensors.

III. EXISTING SYSTEM

- Freire et al. surveyed diverse models of provenance management but did not discuss the use of provenance for security.

- McDaniel addressed that accurate, timely, and detailed provenance information leads to good security decisions.

- Rajbhandari et al. examined how provenance information is associated with a workflow in a Bio- Diversity application.

- Dai et al. proposed a data provenance trust model to evaluate trustworthiness of data and data providers.

- Yu et al. presented an agent-based approach to managing information trustworthiness in network centric information sharing environments.

- Golbeck used provenance information to infer trust in
Semantic Web based social networks.

- Zhou et al. used data provenance computations and queries over distributed streams for effective network accountability and forensic analysis to enhance network security.

Disadvantages

Above studies focused on evaluating trustworthiness in information without considering specific network attack behaviors that may maliciously change the original messages and disrupt system goals.

Secure provenance data

- Hasan et al. insisted that secure provenance is a critical aspect to increase protection of provenance information. Also presented a provenance-aware prototype to ensure integrity and confidentiality of provenance information based on provenance tracking of data writes at the application layer.

- Braun et al. explained that "provenance" consists of
relationships and attributes.

- Wang et al. proposed a "chain-structure" provenance scheme that provides security assurance for provenance meta-data.

- Gadelha and Mattoso proposed a security architecture framework that protects authorship and temporal information in grid-enabled provenance systems.

- Lu et al. proposed a provenance scheme using the bilinear pairing techniques in order to secure provenance data of ownership and process history of data object in cloud computing.

Disadvantages

Above works have studied how to secure provenance data with the existence of a centralized trusted entity. Some researchers have proposed provenance-based trust models in sensor networks, but they assumed full knowledge of the network topology, and did not consider attack behaviors.

IV. PROPOSED SYSTEM

- To propose the use of provenance information for evidence propagation for sparse DTNs without solely relying on encounter-based evidence exchange.

- Unlike existing encounter-based trust protocols, proposed protocol does not require two nodes to exchange trust evidence upon encounter to estimate trust of each other while achieving high trust accuracy by leveraging provenance information embedded in a message during message delivery.

- Leveraging the interdependency of trust in information source and information itself based on the concept of provenance, proposed work a provenance based trust framework, called PROVEST (PROVEnance baSed Trust model).

- In the proposed work, trust is scaled in [0; 1] as a real number, trust evidence, either direct or indirect evidence, is modeled by the Beta distribution with evidence filtering, treating evidence in a Bayesian way, to make PROVEST more generic with the amount of positive and negative evidence.

Advantages

- Minimizes trust bias

- Minimizes communication cost caused by trust assessment; and
- Maximizes quality-of-service (QoS) by minimizing message delivery delay and maximizing correct message delivery ratio.

V. MODULES

- Network Model

- Key management

- Attack model

- Provenance update

(i) Network Model

The nodes interact with each other not only to deliver messages, but also to exchange information for other

purposes. A node is able to diagnose other nodes' attack behaviors based on its past direct experience. A given mission requires that each node, as a source, must send information to a list of destination nodes. Each node, as a destination node (DN), expects to receive information from a set of source nodes (SNs). For message delivery, nodes use the "store-and-forward" technique, meaning that a node carries messages until it encounters a message carrier (MC).

(ii) Key Management

A group communication system in a DTN environment is assumed, where multiple trusted authorities (TAs) exist in the operational area so that a node is allowed to access a TA to obtain a valid symmetric key for group communication. A node encrypts the entire "packet" using a symmetric key KSt given to legitimate members. Note that TAs are only used for group key management, not for trust management or packet routing. These TAs are essential in sparse DTN environments, because contributory group key management with all group members contributing to the group key generation based on Diffie-Hellman key exchange to agree on a secret key will not work in sparse DTN environments. TAs rekey the symmetric key KS;t periodically based on their pre-deployed hash functions. The symmetric keys issued at the same time t by multiple TAs are the same so that all legitimate nodes can communicate with the same key. The symmetric key is used to prevent outside attackers, not inside attackers.

(iii) Attack model

An attack model is designed such that two types of major attacks are considered. One is packet dropping and other is packet modifying. A node may persistently drop packets to perform denial-of-service (DoS) attack. This is considered by a node's persistent packet dropping with the full strength of attack intensity. A node may randomly drop packets to perform random DoS attack. A node's random packet dropping is considered by varying the attack intensity.

(iv) Provenance update

Provenance of node is updated to all its neighbor nodes. When a source node chooses its destination and send packet, the relay which is sending packets is packet modifier, then it may reveal it as a normal node to its neighbor and forward packets. Direct evidence is observed upon every encounter with another node, while indirect evidence is collected when a DN receives a MM enclosing PIs. It is assumed that two nodes can observe each other during their encountering period.

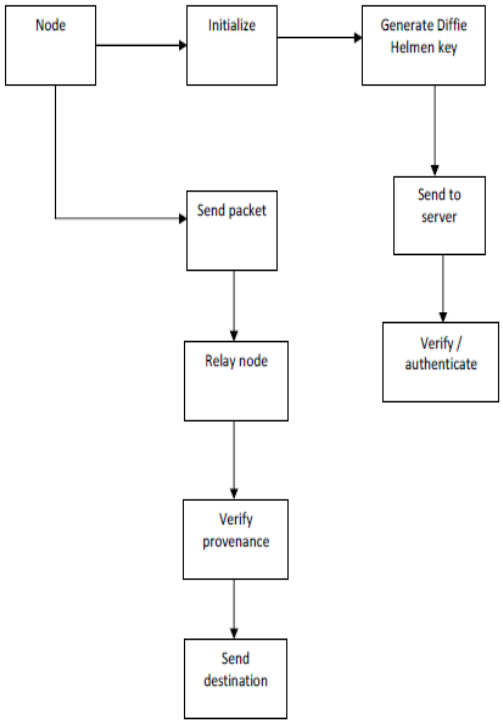
Routing Protocols in DTNs

- Flooding or partial flooding approaches based on connectivity probability have been popularly considered such as Epidemic or PRoPHET. However, these approaches tend to cause network congestion or high interference, and high resource consumption to process and switch operations.
- Opportunistic routing protocols in which a relay node is selected based on certain criteria including historical mobility patterns called RelayCast, a fixed point opportunistic routing using inter-contact times between nodes, and a cluster-based routing protocol for DTNs where a cluster is formed based on similar mobility patterns.

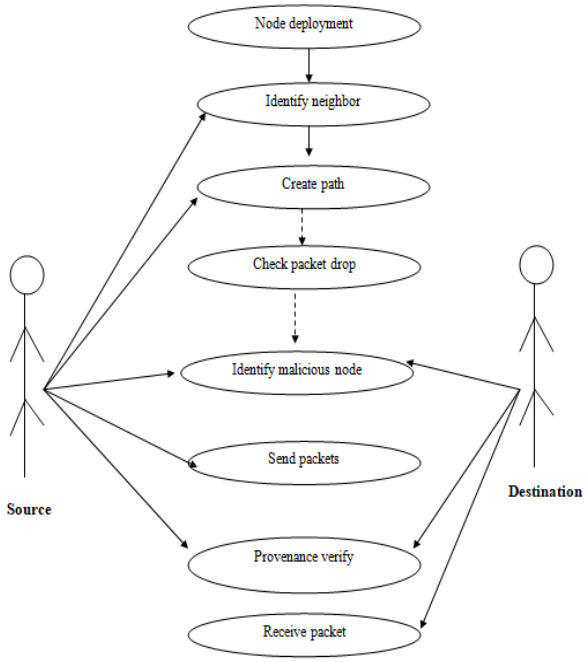
VI. PROBLEM STATEMENT

Managing trust efficiently and effectively is critical to facilitating cooperation or collaboration and decision making tasks in DTNs while meeting system goals such as reliability, availability, quality of service (QoS), and/or scalability. Accurate trust evaluation is especially challenging in DTN environments because nodes are sparsely scattered and do not often encounter each other. Therefore, encounter based evidence exchange among nodes may not be always possible. The lack of direct interaction experience in DTN environments hinders continuous evidence collection and can result in incorrect trust estimation, leading to poor application performance.

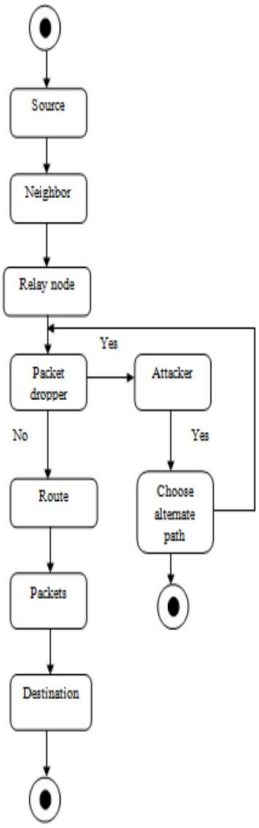
VII. SYSTEM ARCHITECTURE



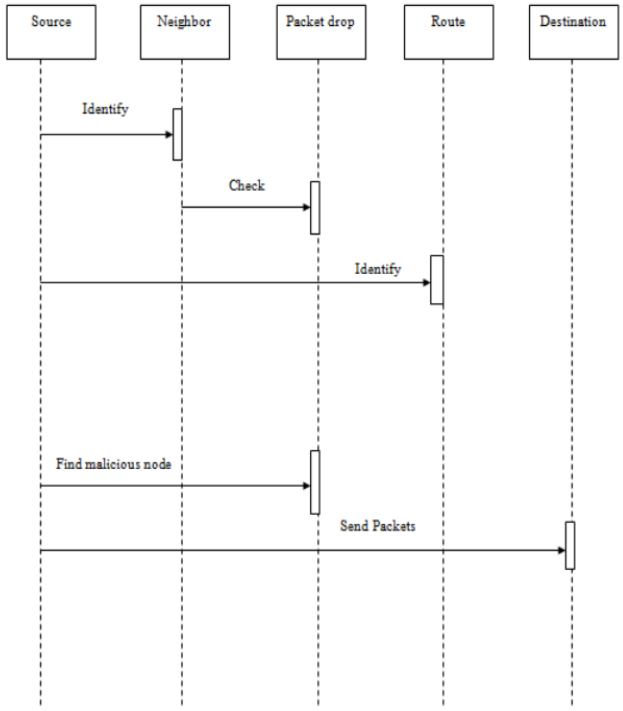
(i)USECASE DIAGRAM



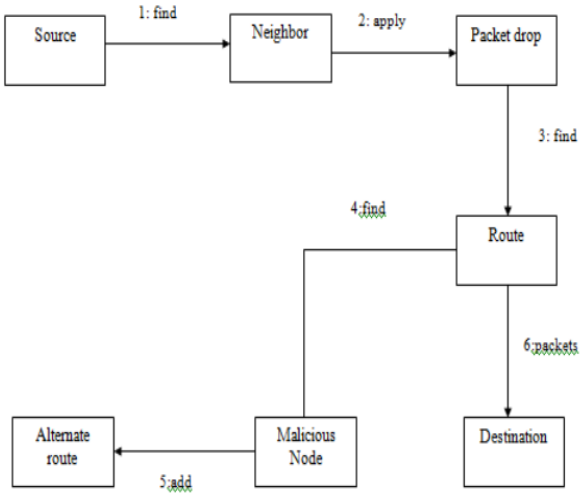
(ii) ACTIVITY DIAGRAM



(iii) SEQUENCE DIAGRAM



(iv) COLLABORATION DIAGRAM



VIII. CONCLUSION

A provenance-based trust model called PROVEST which evaluates trust of a node by leveraging the provenance information added by each intermediate message carrier as indirect evidence during message forwarding. PROVEST performs adaptive control based on the historical pattern of evidence such as positive or negative evidence. This feature excels in identifying bad nodes in the network where trust evidence is uncertain. Provenance-based approach significantly reduces the communication cost while maintaining a high correct message delivery ratio.

IX. REFERENCES

[1] T. Spyropoulos, R. Rais, T. Turletti, K. Obraczka, and A. Vasilakos, "Routing for disruption tolerant networks: taxonomy and design," Wireless Networks, vol. 16, no. 8, pp. 2349–2370, 2010.
[2] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Trust management for encounter-based routing in delay tolerant networks," in IEEE Global Telecommunications Conference, Miami, FL, 6-10 Dec. 2010,pp. 1–6.
[3] "Dynamic trust management for delay tolerant networks and its application to secure routing," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 5, pp. 1200-1210, May 2014.
[4] P. Buneman, S. Khanna, and W. Tan, "Why and where: A characterization of data provenance," in Proceedings of International Conference on Database Theory, Springer- Verlag, 2001, pp. 316–330.
[5] J.-H. Cho, M. Chang, I.-R. Chen, and A. Swami, Trust Management VI, IFIP Advances in Information and Communication Technology. 6th IFIPTM, Surat, India: Springer, 2012, vol. 374, ch. A Provenancebased Trust Model of Delay Tolerant Networks, pp. 52–67.
[6] A. Jøsang and R. Ismail, "The beta reputation system," in Bled Electronic Commerce Conference, Bled, Slovenia, 17-19 June 2002, pp.1–14.
[7] M. Mahmoud, X. Lin, and X. Shen, "Secure and reliable routing protocols for heterogeneous multihop wireless networks," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 1140–1153, March 2015.
[8] L. Moreau, J. Freire, J. Futrelle, R. McGrath, J. Myers, and P. Paulson, "The open provenance model: an overview," in International Provenance and Annotation Workshop, LNCS, vol. 5272, Salt Lake City, Utah, 17-18 June 2008, pp. 323–326.
[9] Y. Liu, J. Futrelle, J. Myers, A. Rodriguez, and R. Kooper, "A provenance-aware virtual sensor system using the open provenance model," in International Symposium on Collaborative Technologies and Systems, Chicago, IL, 17-21 May 2010, pp. 330–339.
[10] J. Freire, D. Koop, E. Santos, and C. Silva, "Provenance for computational tasks: A survey," IEEE Computing in Science and Engineering, vol. 10, no. 3, pp. 11–21, 2008.
[11] P. McDaniel, "Data provenance and security," IEEE Security and Privacy, vol. 9, no. 2, pp. 83–85, 2011.
[12] S. Rajbhandari, I. Wootten, A. Ali, and O. Rana, "Evaluating provenance-based trust for scientific workflows," in 6th IEEE International Symposium on Cluster Computing and the Grid, vol. 1, Singapore, 16-19 May 2006, pp. 365–372.
[13] E. B. C. Dai, Dan Lin and M. Kantarcioglu, "An approach to evaluate data trustworthiness based on data provenance," in Proceedings of 5th VLDB Workshop on Secure Data Management, Lecture Note in Computer Science, vol. 5159, Auckland, New Zealand, Aug. 2008, pp. 82–98.
[14] B. Yu, S. Kallurkar, and R. Flo, "A demspter-shafer approach to provenance-aware trust assessment," in International Symposium on Collaborative Technologies and Systems, Irvine, CA, May 2008, pp. 383–390.
[15] J. Golbeck, "Combining provenance with trust in social networks for semantic web content filtering," Provenance and Annotation of Data, LNCS, vol. 4145, pp. 101–108, 2006.
[16] W. Zhou, E. Cronin, and B. T. Loo, "Provenance-aware secure networks," in IEEE 24th International Conference on Data Engineering Workshop, 2008, pp. 188–193.
[17] R. Hasan, R. Sion, and M. Winslett, "Introducing secure provenance: problems and challenges," in ACM Workshop on Storage Security and Survivability, 2007, pp. 13–18.
[18] U. Braun, A. Shinnar, and M. Seltzer, "Securing provenance," in Proceedings of the 3rd Conference on Hot Topics in Security, 2008, pp. 1–5.
[19] R. Hasan, R. Sion, and M. Winslett, "The case of the fake picasso: preventing history forgery with secure provenance," in Proccedings of the 7th Conference on File and Storage Technologies, 2009, pp. 1–14.
[20] X. Wang, K. Zeng, K. Govindan, and P. Mohapatra, "Chaining for securing data provenance in distributed information networks," in IEEE Military Communications Conference, 2012, pp. 1–6.