Eleyon
SOUTH ASIAN JOURNAL OF ENGINEERING AND TECHNOLOGY

SURVEY ON DELAY TOLERANT NETWORK USING PROVEST SCHEME

Dr.P.Saveetha [a], S.Anisha [b], V.T.Meena [b], S.Pradeep [b], S.Prem [b]

[a] *Associate Professor, Department of Information Technology , Nandha College of Technology, Erode-638052, Tamilnadu, India*

[b] *UG scholar, Department of Information Technology , Nandha College of Technology, Erode-638052, Tamilnadu, India*

[b] *UG scholar, Department of Information Technology , Nandha College of Technology, Erode-638052, Tamilnadu, India*

[b] *UG scholar, Department of Information Technology , Nandha College of Technology, Erode-638052, Tamilnadu, India*

[b] *UG scholar, Department of Information Technology , Nandha College of Technology, Erode-638052, Tamilnadu, India*

***Corresponding Author**
Saveetha.p@nandhatech.org
(Dr.P.Saveetha)
Tel.: +91 9750233555

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[2]. 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.

[1]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[1]. 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[7]. 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[1]. Managing trust efficiently is critical to facilitating cooperation or collaboration and decision making process are done.

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)[1], 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 evidence collection fail to establish routes[11]. 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 networks with large amounts of local storage and internode bandwidth relative to the expected traffic can be cleared and intentionally misbehaving nodes are carred the information.

[2]MODULES

- **Network Model**
- **Key management**
- **Attack model**
- **provenance update**

2.1 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 behaviours 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).

2.2 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 key is used to prevent outside attackers, not inside attackers

2.3 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.

2.4 Provenance update

Provenance of node is updated to all its neighbour 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 neighbour and forward packets[4]. Direct evidence is observed upon every encounter with another node, while indirect evidence is collected when a DN receives a MM enclosing.

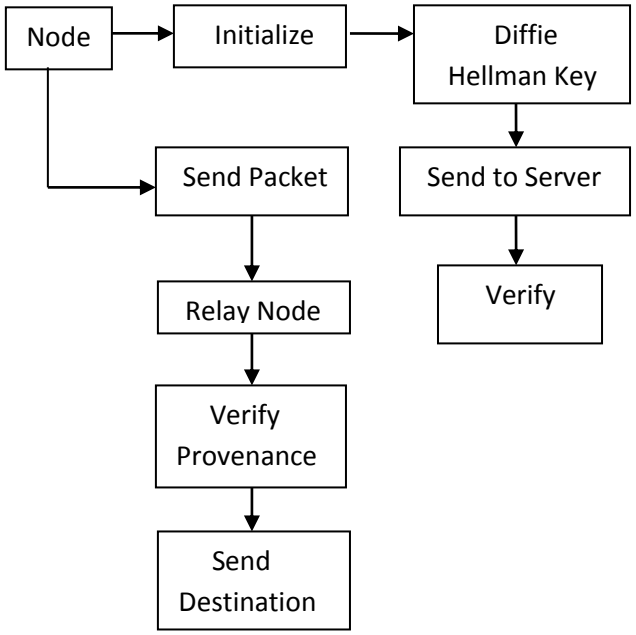

Fig : System Architecture

[3]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[12].
- 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.

Disadvantages

Above studies focused on evaluating trustworthiness in information without considering specific network attack behaviours 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[7]. 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[11].
- 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[9], but they assumed full knowledge of the network topology, and did not consider attack behaviors

[4]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)[3].
- In the proposed work, trust is scaled in [1] as a real number, trust evidence, either direct or indirect evidence, is modeled by the Beta distribution with evidence filtering[6], 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
- Maximizes quality-of-service (QoS) by minimizing message delivery delay and maximizing correct message delivery ratio.

[5]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 reduced communication cost.

[6]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.