IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-7 E-ISSN: 2347-2693

Trust and Security Management Protocol for Delay Tolerant Networks Using Information Centric Network Architecture (ICNA)

M. Arshiya Shajareen* and S.Vasundra

Dept. of Computer Science and Engineering,Jntu A, India.

www.ijcseonline.org

Received: Jun/12/2015 Revised: July/02/2015 Accepted: July/20/2015 Published: July/30/ 2015

***Abstract*— :** Disconnected MANETs have been called as challenged networks and Delay-Tolerant Network (DTN). A DTN provides interoperable communications with and among challenged environments. A challenged network is defined as a network that has one or more of the following characteristics: high end-to-end path latency; end-to-end disconnection meaning a path between a node pair may never exist; limited resources or limited life expectancy either due to lack of battery power, such as in sensor networks, or node damage as may occur in battlefield deployments. Such networks may never have an end-to-end path from source to destination at a given time. Security concerns for delay-tolerant networks vary depending on the environment and application, though authentication and privacy are often critical. The proposed model implements trust and security management protocols for delay tolerant and self contained message forwarding applications based on information centric networks architecture. Further, it is aimed to test the dynamic trust management protocol design on other trust based DTN applications for showing better utility of the algorithm.

***Keywords*—**Verification and Validation; Delay Tolerant Networking; Secure Routing; Performance Analysis

I. INTRODUCTION

Routing in delay tolerant MANETs is challenging because these networks may never have an end-to- end path from source to destination at a given time. Due to the existence of long delay paths, frequent disconnections and network partitions, information may be carried by a mobile node and forwarded opportunistically across partitions, therefore allowing communication between areas of the network that are never connected by an end-to-end path.

A. Security in Decentralized and Open Environment:

Security can be viewed from a centralized or decentralized perspective. Each of these perspectives introduces various security challenges since their properties and environments differ. One of the main properties of a centralized security system is that a single pivotal point exists, from which security can be marshaled, co-ordinate and managed. In a decentralized security system, however, a single pivotal point does not exist. Indeed many such points will co-exist. Two types of environment can be classified,

- Closed and
- Open environments.

A closed environment is one in which tight control exists over a number of issues such as systems, users, resources and infrastructure. An open environment can be seen as a more liberal environment where each component in the environment is to an extent free of one another. For example, the Windows operating systems can be regarded as systems designed in a closed environment with little or no input from external sources. The Linux operating systems are designed in open environments where anyone from anywhere can, in principle, input into the design and direction of the system. A key advantage of open environments is their collaborative nature. This is not to say that collaboration does not exist in closed environments.

B. Security Concepts:

Security is a broad topic of research but some principle concepts are worth mentioning here. This is not to disregard other concepts or other aspects of security, but rather to emphasize those that underpin this thesis. The concepts shown in Figure 1 include: Authentication, Authorization, Confidentiality, Integrity and Non-repudiation. The concept of trust is also discussed in this section, since it underpins each of these concepts.

Authentication:

Authentication is the identification and assurance that a subject is who they claim to be. It is the assertion of the ownership of an identity. A subject's identity is usually verified when a proof of identity is provided.

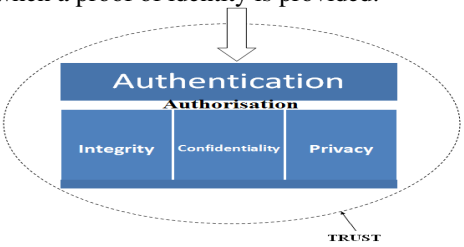


Figure 1: Trust and Security Concepts

For example, an identity may be proved or verified when a username and pass phrase are presented and successfully validated against a stored phrase or key. Alternatively an identity may be verified when a valid digital certificate is presented along with data signed by the subject [2, 3]. Usually the certificate is signed by a mutually trusted third party and the certificate binds the identity of a subject to their public-key. A parallel example of a digital certificate is a driver's license or passport.

Authorization: Authorization is the validation that a subject has the required privileges to access a resource. Usually authorization is achieved through some sort of access control policies, restricting access to protected resources for privileged users or entities. An access policy primarily indicates what actions a subject is authorized to perform on an object or the capabilities of a subject in a system. It typically defines the context, attributes and constraints that must be satisfied before access can be granted to an object. Today, numerous authorization models are in use often based on one or more policy specifications. Some of the policy specifications that exist today include: discretionary, mandatory and role-based policies. These policies are discussed in more detail in [4], while [5] compares and contrasts centralized and decentralized authorization models. An assumption made by most authorization models is that a subject's identity has been validated prior to the system deciding access control. Thus it is always required that a subject is authenticated before he or she can be authorized.

Confidentiality: Is the assurance that information either stored or in transit can only be accessed by authorized entities. Using cryptographic techniques, confidentiality can be improved to protect against man-in-the-middle attacks [6], but can be compromised where the shared key or private key are exposed, for example. In some cases, both shared key and public-key cryptography are used to achieve better performance. Today, technologies such as HTTPS using Transport Layer Security (TLS) [7] provide secure point-to-point connection through which data can be transmitted securely between endpoints. However, when intermediary parties such as proxies need to access and work on data being transmitted, TLS does not ensure end-to-end security. End-to-end security ensures that a message or parts of a message are encrypted and can only be viewed by the intended recipient regardless of the nature of connection or intermediaries that are required to work on parts of the message. As such, technologies using Message Level Security (MLS) [8] are often preferred for confidentiality since they ensure end-to-end security.

Integrity: Is the assurance that an unauthorized modification of data has not occurred in transit or generally. This implies that anyone should be able to read or make use of the data with certainty that the data has not been tampered with or altered by an unauthorized entity. Encrypting data with a private-key ensures that only the person with private-key can modify it while others with the associated public-key can read or open it. In practice, for performance reasons, it is normally the case that the digest of the message is taken and encrypted with the private-key. The recipient receives the digest and decrypts the encrypted digest with the public-key. The decrypted digest is then compared with the received message to verify the message integrity. Message digests are created using a checksum or one-way hash algorithms such as MD5 (128-bit hash value) or SHA-1 (160-bit hash value) [9]. Reliability of these hash algorithms against attacks depend on the size (in bits) of the hash values.

Non-repudiation: Non-repudiation is the assurance those transactions once performed by a subject are undeniable. This is a requirement that cryptography by itself cannot satisfy. Non-repudiation requires the generation, verification, storage and tracking of evidence and facts in order to resolve disputes that may arise. Usually the process of dispute resolution involves trusted third parties that validate tracked and stored evidence such as certificates, signatures, transaction details and time stamps.

Trust: Trust is the underlying phenomenon of security concepts. Trust is built on the concept of limiting expected behavior [10]. It is associated with an assurance measurement. The level of confidence in limiting behavior within a security context determines the level of assurance. From an authentication point of view, trust defines the level of assurance that should be associated with identity. From an authorization point of view, trust defines the expected behavior of an entity in possession of security credential, i.e. what the entity should have access to or what privileges they can have. From a confidentiality point of view, trust is the assurance or confidence associated with behavior, e.g. the confidence in certain entities to keep information secured and protected. From an integrity point of view, it is the assurance of an expected behavior. For non-repudiation, it is the assurance that an action or behavior is undeniable.

II. RELATED WORK

Marsh [11] is among the first who tried to develop formalization for trust as a computational concept. In Marsh's formalization, trust is separated into three different categories: basic, general, and situational trust, with each represented by a value in (-1, 1). Basic trust represents the general trust disposition of the trustor, not in any specific situation or toward any specific trustee. It is derived from past experience with all other agents in all situations, through the entire life of experiences. General trust represents the trust toward a specific trustee, but not in any specific situation. Situational trust represents the trust toward a specific trustee in a specific situation. They formalized situational trust as the product of three parts: utility that can be gained from the situation, importance of the situation to the trustor, and general trust. They also introduced the temporal index into the formalization to

represent evolving trust over time. The formalization provides a description of trust and is large in the sense that extensions are possible [11]. Nevertheless, the limitations of the formalization, as discussed in their work, are (a) the range value selected for trust (-1, 1) is problematic (e.g., the product of two negative trust values is positive), and (b) the operators for the formalization are limited.

There are many computational trust models being proposed in the literature, including

- weighted summation,
- Bayesian,
- game theory based, and
- Information theory-based models.

A.Weighted Summation Models

One of most popular and straightforward computational trust models is the weighted summation or average model [12]. Models in this category aggregate trust using a weighed calculation on information collected from different sources (e.g., direct observation vs. indirect observation [13], past experience vs. recent experience, etc.). The weight parameters are determined by factors such as the trustworthiness of the information provider, the rate of trust decay, etc. For example, eBay employs this model to calculate the feedback score. The advantages of this kind of models are, first it is simple and easy to understand, and second the linear calculation is easy to implement and efficient. However, it is a challenge to find the best weight parameters to achieve an accurate trust evaluation.

B. Bayesian Models

In Bayesian trust models, the evidence of trust is considered as a stochastic process. First, a prior distribution of the trust value is assumed. Then, the evidence is observed and can be used as the likelihood to calculate the posterior distribution following Bayes' Theorem. After new evidence is observed, the previous posterior distribution obtained can be used as a new prior distribution to calculate the next posterior distribution iteratively. The new evidence could be from direct observations or indirect recommendations. Direct observations may be used to update the numbers of positive and negative interaction experiences, whereas indirect recommendations may be discounted by the confidence or belief [14] of the trustor toward the recommenders. Iterative computing process, it is desirable if both the prior and posterior distributions follow the same distribution and only the parameters are updated iteratively after new evidence is observed.

C. Game Theory Models

Game theory based trust models [15] usually use incentives to stimulate the cooperation between nodes, such that the system can reach a stable state where the overall utility is maximized. However, these models only consider selfish nodes and cannot deal with malicious nodes that intend to disrupt the system functionality. Staab, et al. [16] proposed a trust model by considering a game between normal nodes and attackers, given the knowledge of the strategies that attackers will use in each system configuration. Their model can be used to find the optimal parameters for an evidence based trust model to maximize the expected utility. However, in reality, it is difficult to obtain a complete set of attacker strategies and the attacker behavior may change dynamically.

D. Information Theory Models

In information theory models [17], trust is considered as a measure of certainty of whether the trustee will perform an action in the trustor's point of view. Depending on the way of aggregating trust, there are two trust models: entropy-based and probability based. In the entropy-based trust model, trust is calculated as the entropy of information (recommendations) from others. In the probability-based model, trust is obtained by aggregating recommendations using conditional probability. Similar to Bayesian trust management, information theory models do not have direct trust vs. indirect trust as design parameters and only address trust aggregation protocol design.

E. Trust Management in Delay Tolerant Networks

Because of the sparse connection of DTNs, trust management proposed for traditional MANETs are not directly applicable to DTNs. Xu et al. [17] proposed a trust management scheme for secure routing in DTNs. Their protocol considers three sources to estimate trust: cryptographic operation, node's behavior, and reputation. For cryptographic operations, encryption and decryption mechanisms are used to provide authentication and confidentiality and to defend outside attackers. A watchdog mechanism is adopted to detect node's behavior, i.e., whether a neighbor node has successfully forwarded a message or not. The information obtained from cryptographic operation and node's behavior is combined using weighted summation to generate a local trust value. Each node also exchanges its local trust evaluation as recommendation to others. A limitation of their work is that, they did not consider insider attacks from compromised nodes that already have the secret information for encryption and decryption. Another issue is that in DTNs, a node usually has little chance to observe the behavior of next message carrier because of the sparse connectivity and store-and-forward routing mechanism.

Ayday et al. [18] designed an iterative trust management scheme for DTNs. They employed the authentication technique as the underlying mechanism to evaluate a node. A node exchanges its trust evaluation with others and interactively updates its trust evaluation. Inconsistent trust evaluations are identified and removed iteratively until the trust evaluation converges. However,

the iteration process has to be performed on each node every time trust is updated, which is inefficient and time-consuming for mobile networks with a large number of nodes. There is very little research to date on the social aspect of trust management for DTNs. Social relationship and social networking were considered as criteria to select message carriers in a DTN . However, no consideration was given to the presence of malicious or selfish nodes. Li et al. [19] considered routing by socially selfish nodes in DTNs, taking into consideration the willingness of a socially selfish node to forward messages to the destination node because of social ties. However, their protocol assumes a social connection graph is known and uses this graph to facilitate trust evaluation. Such information may not be available as input especially for military operations.

III PROPOSED TRUST MODEL

This paper aims to implement the trust model defined in [1] to the information centric architecture model. The trust management is done under the message passing between every node and transmission of data between the trusted nodes.

A. Trust Composition:

For designing trust composition this system considers two types of trust properties:

- **QoS trust:** QoS trust is evaluated through the communication network by the capability of a node to deliver messages to the destination node. We consider "connectivity" and "energy" to measure the QoS trust level of a node.
- **Social trust:** Social trust is based on honesty or integrity in social relationships and friendship in social ties. We consider "healthiness" and social "unselfishness" to measure the social trust level of a node.

The selection of trust properties is application driven. In DTN routing, message delivery ratio and message delay are two important factors. This system considers "healthiness", "unselfishness", and "energy" in order to achieve high message delivery ratio, and we consider "connectivity" to achieve low message delay.

The trusted authority node sends a RREQ as shown in figure 2 to all the nodes and the nodes which send reply to this RREQ are considered for trust composition.

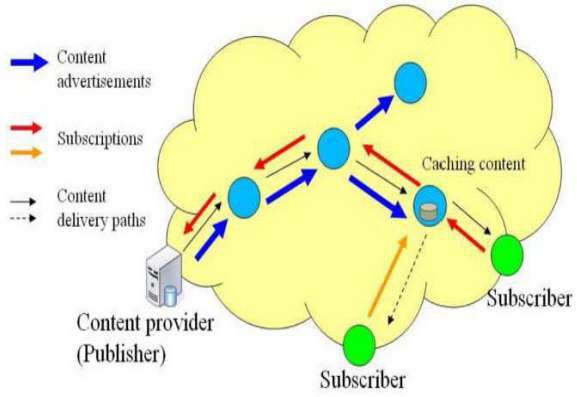
B. Trust Formation:

This paper defines a node's trust level as a real number in the range of [0, 1], with 1 indicating complete trust, 0.5 ignorance, and 0 complete distrust. This system considers a trust formation design (described in the middle part of Fig) by which the trust value of node j evaluated by node i at time t, denoted as $T_{i,j}(t)$, is computed by a weighted average of healthiness, unselfishness, connectivity, and energy.

The intermediate nodes send a report about the current condition of them to the trusted party as shown in figure 3. If the reports reach the trusted party then the nodes will be considered to participate in trust formation.

C.Information Centric Architecture:

The above all the modules are deployed in an Information Centric Architecture. In the information-centric paradigm, the principal concern of the network is to expose, find and deliver information rather than the reachability of end-hosts and the maintenance of conversations between them. Another key principle that comes with the interest-oriented networking in the ICN paradigm is the use of dynamic content caching to enable fast, reliable and scalable content delivery with maximized bandwidth to avoid congestion.



After the trust formation, if the trusted party doesn't get any reports from any node then the trusted party (TP) asks that specific node to send a report individually as show in figure 5. If that node fails to send the report then that node will be considered as cheating node and eliminated from the network and based on the energy levels of the nodes a minimum number of Trusted nodes are categorized and messages are transmitted from source to destination only through these trusted nodes as depicted in figure 6.

Finally only the trusted nodes will be able to transmit the data. Without the trust formation the data will not be transmitted to any other intermediate nodes.

IV ANALYSIS

Every Routing algorithm has to be tested for various performance evaluations. The proposed algorithm is also tested under NS2.35 for the various performance metrics which include:

- Packet Drops
- Packet Delivery Ratio

- Through Put
- Evidence Aggregation

The metrics depicted above are the crucial measurements in any routing procedures. For comparisons the trust aggregation metric uses the existing system [1] and traditional AODV routing protocol.

The first metric is the Packet drop. The analysis is depicted in figure 7.The figure clearly shows that there are no packets drops are occurring in the proposed system. This is due to that the messages are transmitted only through the trusted Nodes.

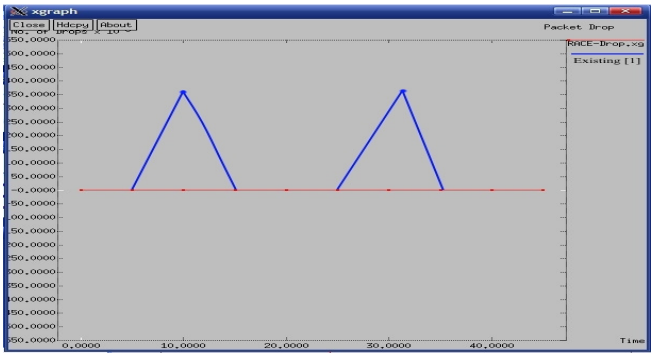


figure 7:packet drop

The figure 8 depicts the packet delivery ratio and the ratio of delivering the packets is almost complete. This means all the packets are delivered completely without any loss of information. The next aspect is the throughput any network performance is depicted by this throughput metric. Figure 9 depicts this analysis result.

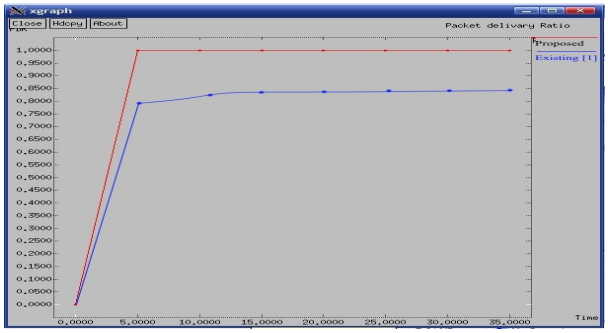


Figure 8: Packet Delivery Ratio

The final metric is the trust aggregation; this trust aggregation is the main aspect of any ICA, where the trusts of the nodes are aggregated. The number of evidences gathered must be maximum with the ratio to the packets stored. Figure 10 depicts these results.

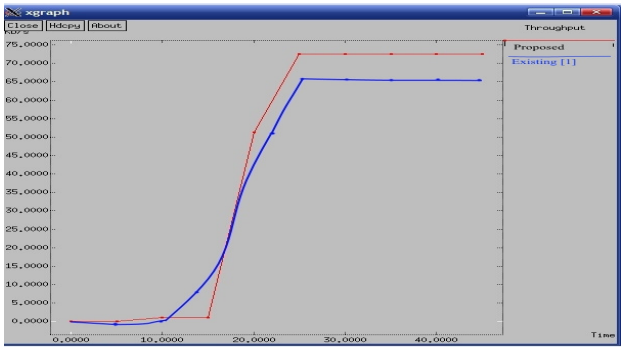


Figure 9: Throughput

As the results clearly show that the aggregation of the proposed system is higher than both the Existing and traditional AODV routing.

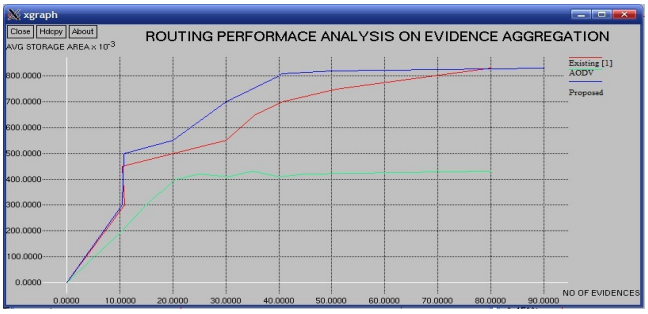


Figure 10: Evidence Aggregation

V.CONCLUSION:

Based on the design and validation principles of dynamic trust management, this paper has addressed trust composition by exploring both social trust and QoS trust metrics, and proposed trust aggregation and trust propagation protocols for DTNs. Further the proposed method used the Information Centric Architecture where the nodes randomly communicate with each other and transmits the information about the trust aggregation and trust composition properties. The analysis provided proves that the trust aggregation has been improved to greater extent compared to the existing system.

REFERENCES

[1] Ing-Ray Chen, Fenye Bao, "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 5, MAY 2014, pp.1200-1210.

[2] W. Stallings, Network Security Essentials: Applications and Standards. Prentice Hall Pearson Education Inc., 2003.

[3] P. Windley, Digital Identity. O'Reilly, 12, Aug. 2005.

[4] R. S. Sandhu and P. Samarati, \Access Control: Principles and Practice," IEEE Communications Magazine, vol. 32, no. 9, pp. 40{48, 1994.

[5] R. Sinnott, D. W. Chadwick, T. Doherty, D. Martin, A. J. Stell, G. Stewart, L. Su, and J.Watt, \Advanced Security for Virtual Organisations: Exploring the Pros and Cons of Centralised vs Decentralized Security Models," in 8th IEEE International Symposium on Cluster Computing and the Grid (CCGrid), Lyon, France, May 2008, May 2008.

[6] T. Dierks and E. Rescorla, \The Transport Layer Security (TLS) Protocol Version 1.1." Request for Comments RFC 4346, April 2006.

[7] S. Shirasuna, A. Slominski, L. Fang, and D. Gannon, \Performance Comparison of Security Mechanisms for Grid Services," in GRID '04: Proceedings of the Fifth IEEE/ACM International Workshop on Grid Computing, (Washington, DC, USA), pp. 360{364, IEEE Computer Society, 2004.

[8] National Institute of Standards and Technology, Secure Hash Standard (SHS), FIPSPUB 180-1." http://www.itl.nist.gov/_pspubs/_p180-1.htm, 1995. (Visited December 2008).

[9] M. Benantar, Access Control Systems: Security, Identity Management and Trust Models. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005.

[10] S. P. Marsh, “Formalising Trust as a Computational Concept,” Department of Computing Science and Mathematics, University of Stirling, Stirling, UK, 1994.

[11] E. Aivaloglou, and S. Gritzalis, “Trust–Based Data Disclosure in Sensor Networks,” IEEE International Conference on Communications, 2009, pp. 1-6.

AUTHORS PROFILE

M.ARSHIYA SHAJREEN received B.Tech degree in Computer Science and Engineering from Intell Institute of Engineering and Technology Anantapur, affiliated to JNTUA University, Anantapuramu, A.P, India, during 2009 to 2013. Currently pursuing M.Tech in Computer Science(Software Engineering) from JNTUA College of Engineering, Anantapuramu, A.P, India, during 2013 to 2015 batch. Her Area of interests include Network Security,Network Architecture.

Dr S. VASUNDRA, presently working as Professor and Head of the Department CSE, JNTUA CEA. She completed her Ph.D from JNTUA university, anantapur, M.Tech from JNTUA and B.E from VTU. She is having 16 years of teaching experience and 5 years of research experience. Published 20 papers in various international journals and 3 in national journals. Her areas of interest include MANET’s, Cloud Computing, Algorithms, Data Structures and Distributed Computing.

.