DYNAMIC TRUST AND SECURITY MANAGEMENT PROTOCOL FOR DELAY TOLERANT NETWORKS

Mrs. Suvarna L. Kattimani[1], Mr. Jaeerahmad N. Indikar[2], Dr Suvarna Nandyal[3]

[1]Assistant Professor, [2]PG Scholar, [3]Professor, HOD, Dept of CSE,
BLDEA'S Dr Halkatti College of Engineering & Technology, Vijayapur, Karnataka, (India)

ABSTRACT

Delay tolerant networks (DTNs) are depicted by high frequent disconnection, end-to-end latency, and opportunistic communication over unreliable wireless links. To avoid these anomalies we propose a dynamic trust & security management protocol for secure routing optimization in DTN environments in the presence of well-behaved, selfish and malicious nodes. Which will be a novel model-based methodology for the analysis of our trust protocol and validate it via simulation, we address dynamic trust and security management using the information centric networks (ICN) architecture, i.e., determining and applying the best operational settings at runtime in response to dynamically changing network conditions to minimize trust bias and to maximize the routing application performance. The results demonstrate that our protocol is able to deal with selfish behaviours and is resilient against trust-related attacks comparison to Bayesian trust-based routing protocols, Dynamic trust and security management without ICN architecture and with using ICN architecture .Furthermore, our trust and security based routing protocol can effectively trade off message overhead and message delay for a significant gain in delivery ratio.

Keywords: DTN, DTSMP, ICN

I. INTRODUCTION

Mobile network typically consist of many heterogeneous nodes performing end-to-end wireless communications to achieve the system functionality. There are various types of mobile networks, including delay/disruption tolerant networks (DTNs) [9] ,mobile ad-hoc networks (MANETs) [11], Internet of things (IoT) systems [5] ,mobile wireless sensor networks (WSNs) [4] etc. The key features of mobile networks are low dependency on infrastructure, no centralized entity needed for managing the network (distributed control), and change of network topology, population size, etc (dynamic). Because of these main features, mobile networks have been widely deployed in many applications. For example, conference attendees can set up an ad-hoc network using their laptops for discussion instant messaging. In war situations, a soldier can dynamically assemble and manage a mobile network consisting of group members to achieve a critical mission assigned. In zoology research, sensors can be attached to wild animals to form a delay tolerant WSN in order to track animal behaviors.

Trust management in mobile wireless network is always been challenging because of frequently changing network environment. This will cause delay tolerance networks (DTN) a high latency, frequent disconnection over unreliable wireless links. Many researchers worked and designed and validate the Trust management for delay tolerant networks (DTN).

The contribution of the paper related to the some of the existing work in trust management for DTNs which are summarized as follows

1. We have combined the social trust and quality of service which are derived from social network and communication network respectfully. We have used the two social trust metrics called "unselfishness" and "healthiness" to find the both malicious and socially selfish nodes in the DTN environment.
2. We address the issue of the trust based DTN routing through dynamic trust and security management protocol by adjusting trust protocol setting dynamically for the changing DTN environment.
3. We deploy trust and security management protocols for delay-tolerant, self-contained message forwarding applications based on the information-centric networks (ICN) architecture.
4. We perform comparative analysis of trust and security management protocol with respective the Bayesian trust-based routing protocols and Dynamic trust and security management protocol using ICN.

II. RELATED WORK

2.1 Computational Trust Models

There are many computational trust models being proposed in the literature, including Bayesian [14], weighted summation [3], game theory based [7], fuzzy logic based [8], routing algebra based [19], graph based [18],belief based, flow based [6] , and information theory-based [10] models. Below we survey and contrast our work with the first three computational trust models which have been used most frequently in the literature.

2.1.1 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 [12] or belief [15] of the trustor toward the recommenders. Since this is an 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. Therefore, conjugate prior distributions, like Beta distribution [14] and Dirichlet distribution [14] are usually used as the prior distribution to build trust models.

2.1.2 Weighted Summation Models

One of most popular and straightforward computational trust models is the weighted summation or average model [2,3]. Models in this category aggregate trust using a weighed calculation on information collected from different sources (e.g., direct observation vs. indirect observation [3], 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 [16] 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. Our dissertation research considers weighted summation as one of the many possible ways for trust formation and it seeks the best trust composition and formation to maximize application performance.

2.1.3 Game Theory Models

Game theory based trust models [7] 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. [13] 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. In our dissertation research we do not make assumptions of the attacker strategies. Rather, we design dynamic trust management protocols that can learn from past experiences and adapt to changing environment conditions to maximize application performance and enhance operation agility.

2.1.4 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. In our dynamic trust management, we consider the design of trust composition, trust propagation, trust aggregation and trust formation protocols.

2.2 Information centric networks (ICN) architecture.

Information-Centric Networking (ICN) has emerged as a promising candidate for the architecture of the Future Internet. Inspired by the fact that the Internet is increasingly used for information dissemination, rather than for pair-wise communication between end hosts, ICN aims to reflect current and future needs better than the existing Internet architecture. By naming information at the network layer, ICN favours the deployment of in-network caching deployment of in-network caching (or storage, more generally) and multicast mechanisms, thus facilitating the efficient and timely delivery of information to the users. However, there is more to ICN than information distribution, with related research initiatives employing information-awareness as the means for addressing a series of additional limitations in the current Internet architecture, for example, mobility management and security enforcement, so as to fulfil the entire spectrum of Future Internet requirements and objectives.

Survey papers exist for research in the Future Internet area (e.g., [27] and [28]), due to their broad coverage they treat ICN architectures and related research efforts either sketchily or incompletely. The aim of this survey is to focus on ICN and cover the state-of-the-art evenly, broadly, and at some depth. Compared to other ICN surveys (e.g. [29] and [30]) the present survey covers in more detail and depth the most representative and mature ICN architectures and approaches, instead of a subset. In addition to describing the goals and basic concepts of the various research projects on ICN, it identifies the core functionalities of all ICN architectures and highlights their similarities and differences in how these functionalities are implemented. Furthermore, it provides a critical analysis of the main unresolved research challenges in ICN that require further attention by the community.

III. SYSTEM MODEL

We design a DTN environment with no centralized trusted authority. Nodes communicate through multiple hops. When a node encounters another node, they exchange encounter histories certified by encounter tickets so as to prevent black hole attacks to DTN routing. We differentiate socially selfish nodes from malicious nodes. A selfish node acts for its own interests including interests to its friends, groups, or communities. So it may drop packets arbitrarily just to save energy but it may decide to forward a packet if it has good social ties with the source, current carrier or destination node. We consider a friendship matrix to represent the social ties among nodes. Each node keeps a friend list in its local storage. A similar concept to the friendship relationship is proposed in [26], where familiar strangers are identified based on colocation information in urban transport environments for media sharing. Our work is different from [26] in that rather than by frequent colocation instances, friendship is established by the existence of common friends. Energy spent for maintaining friend lists and executing matching operations is negligible because energy spent for computation is very small compared with that for DTN communication and matching operations are performed only when there is a change to the friend lists. When a node becomes selfish, it will only forward messages when it is a friend of the source, current carrier, or the destination node, while a well-behaved node performs altruistically regardless of the social ties. A malicious node aims to break the basic DTN routing functionality. In addition to dropping packets, a malicious node can perform the following trust-related attacks:

1. **Self-promoting attacks:** it can promote its importance (by providing good recommendations for itself) so as to attract packets routing through it (and being dropped).
2. **Bad-mouthing attacks:** it can ruin the reputation of well-behaved nodes (by providing bad recommendations against good nodes) so as to decrease the chance of packets routing through good nodes.
3. **Ballot stuffing**: it can boost the reputation of bad nodes (by providing good recommendations for them) so as to increase the chance of packets routing through malicious nodes (and being dropped).

A malicious attacker can perform random attacks to evade detection. We introduce a random attack probability P(rand) to reflect random attack behavior. When P(rand) <1, the malicious attacker is a reckless attacker; when P(rand) < 1 it is a random attacker.

A collaborative attack means that the malicious nodes in the system boost their allies and focus on particular victims in the system to victimize. Ballot stuffing and bad-mouthing attacks are a form of collaborative attacks to the trust system to boost the reputation of malicious nodes and to ruin the reputation of (and thus to victimize) good nodes. We mitigate collaborative attacks with an application-level trust optimization design by setting a trust recommender threshold Trec to filter out less trustworthy recommenders, and a trust carrier threshold Tf to select trustworthy carriers for message forwarding. These two thresholds are dynamically changed in response to environment changes.

A created for the Application Developers, Enabling them to build and test the system. Many organizations look at System Design primarily as the preparation of the system component specifications; however, constructing the various system components is only one of a set of major steps in successfully building a system. The preparation of the environment needed to build the system, the testing of the system, and the migration and preparation of the data that will ultimately be used by the system are equally important. In addition to designing the technical solution, System Design is the time to initiate focused planning efforts for both the testing and data preparation activities.

Software design is an important activity in SDLC (Software Development Life Cycle). This is the third activity that emphasize on the requirements that are analyzed in Requirement Analysis Phase by building models that provides initial glimpse of what the real system looks like. Some of the software development activities are.

- Planning
- Implementation
- Testing and Documentation
- Deployment

IV. DYNAMIC TRUST AND SECURITY MANAGEMENT PROTOCOL (DTSMP)

4.1 DTSMP

Our trust and security protocol considers trust composition, trust aggregation, trust formation and application-level trust optimization designs. Figure 1 shows a flowchart of our trust management protocol execution. For trust composition design (described in the top part of Figure 1), we consider two types of trust properties:

- *QoS trust*: QoS trust [22] 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. The connectivity QoS trust is about the ability of a node to encounter other nodes due to its movement patterns. The energy QoS trust is about the battery energy of a node to perform the basic routing function.
- *Social trust*: Social trust [22, 25] 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 healthiness social trust is the belief of whether a node is malicious. The unselfishness social trust is the belief of whether a node is socially selfish. While social ties cover more than just friendship, we consider friendship as a major factor for determining a node's socially selfish behavior.

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

We define 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. We consider a trust formation design (described in the middle part of Figure 1) 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 as follows:

$$T_{i,j}(t) = \sum_{X}^{all} W^X \times T_{i,j}^X(t)$$

where X represents a trust property explored ðX ¼ healthiness, unselfishness, connectivity or energy), Tx is node i's trust in trust property X toward node j, and wX is the weight associated with trust property X with the sum equal to 1. wX is application-dependent. However, it is not related to the application priority [22] but dependent on the operational profile of an application [23]. We aim to identify the best weight ratio under which the application performance (secure routing) is maximized, given an operational profile [23] as input. Before this can be achieved, however, one must address the accuracy issue of trust aggregation. That is, for each QoS or social trust property X, we must devise and validate the trust aggregation protocol executed by a trustor node to assess X of a trustee node such that the trust value computed is accurate with respect to actual status of the

trustee node in X. This is achieved by devising a trust propagation protocol (described in the middle part of Fig. 1) with tunable parameters which can be adjusted based on each trust property.

The design principles of DTN-ICN are described below:

1. We design the service abstraction that is provided to applications by defining an information model, as well as a service model, that is exposed to them. We utilise existing DTN and ICN solutions as a basis for this common abstraction, providing an object-level graph-based information abstraction. Information is split into several items or objects and each such object is associated with a context (also known as scoping). Scope represents sets of information. Both information objects a nd scopes are represented as directed acyclic graphs (DAG) manipulated through a set of publish/subscribe operations. While we expect applications to natively utilise this common information-centric interface of the architectural framework, we also foresee interfaces being defined that allow, or example, socket emulation [21] that would enable backward compatibility.
2. We functionally decompose the network components using PURSUIT ICN and existing DTN (Bundle Protocol [20]), into three core functions, namely rendezvous, topology management and forwarding. The functional decomposition also addresses the interaction with the underlying networks, such as satellite, cellular, WiFi or optical networks. This is accomplished mainly through the topology management function, which manages the resources available in the form of links, spectrum, wavelength but also storage and computational capability.

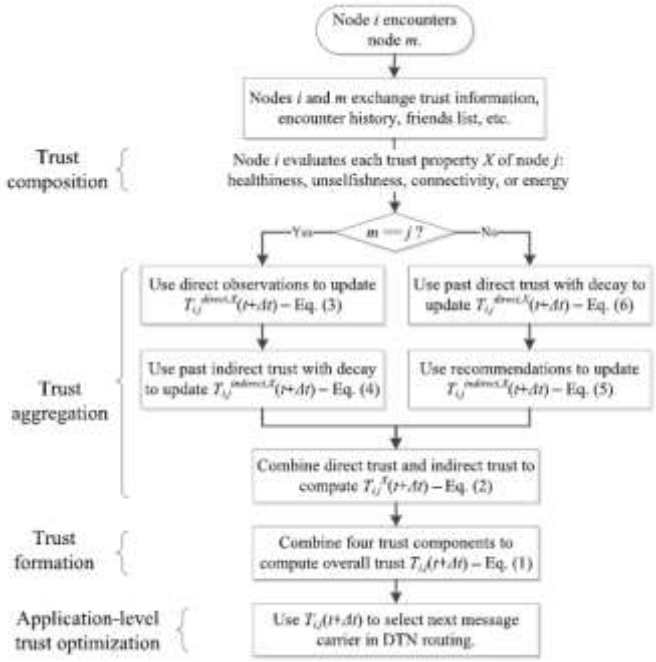

Figure 1: A Flowchart for Trust Protocol Execution.

3. Based on our decomposition, we define the interfaces between the core components of our architectural framework, e.g., for initiating discovery requests, assembling network resources for store-and-forward operations or forwarding information objects over paths that were assembled through the topology management function. These interfaces are realised through various dissemination strategies that enable traversal across the various connectivity options, e.g., over challenged and opportunistic network environments (using DTN), IP-based backhauls (IP being used as a 'framing' (link layer) based backhauls (IP being used as a 'framing' (link layer) protocol) or using native ICN for high speed optical links.

V. RESULTS

5.1 Simulation Setup

As in our paper we going to compare the three protocols Bayesian, DTM and DTM-ICN for each protocol the simulation setup is explained as follows.

Bayesian Trust protocol: The simulation parameter for Bayesian is as shown in Table 5.1. A single scenario comprising of 30 mobile nodes moving at a variable speed from 5 meter per seconds to 25 meter per second. The number of node can be select explicitly and even the mobility (m/s) can be set explicitly, Simulation time was taken 1000 seconds. Simulation area taken is 1500 x 300 meters. Packet Inter-Arrival Time (sec) is taken exponential (1) and packet size (bits) is exponential (1024). The data rates of mobile nodes are 11 Mbps with the default transmitting power of 0.175 watts. Random way point mobility is selected.

DTM Protocol: The simulation parameter for DTM is as shown in Table 5.2. A single scenario comprising of 30 mobile nodes moving at a variable speed from 5 meter per seconds to 25 meter per second. The number of node can be select explicitly and even the mobility (m/s) can be set explicitly, Simulation time was taken 1000 seconds. Simulation area taken is 1500 x 300 meters. Packet Inter-Arrival Time (sec) is taken exponential (1) and packet size (bits) is exponential (1024). The data rates of mobile nodes are 11 Mbps with the default transmitting power of 0.175 watts. Random way point mobility is selected.

DTM-ICN: DTM Protocol: The simulation parameter for DTM-ICN is as shown in Table 5.3.A single scenario comprising of 32 mobile nodes moving at a variable speed from 5 meter per seconds to 25 meter per second where 2 nodes act as servers in topology. The number of node can be select explicitly and even the mobility (m/s) can be set explicitly, Simulation time was taken 1000 seconds. Simulation area taken is 1500 x 300 meters. Packet Inter-Arrival Time (sec) is taken exponential (1) and packet size (bits) is exponential (1024). The data rates of mobile nodes are 11 Mbps with the default transmitting power of 0.075 watts. Random way point mobility is selected.

SIMULATION PARAMETERS	
Examined Protocols	Bayesian
Simulation Time	1000 seconds
Simulation Area(MxM)	1500x300
Number Of Nodes	30
Traffic Type	UDP
Performance Parameter	Average delay, Packet Delivery ration, Packet Energy, Packet overhead
Initial Energy (joules)	100 joules
Mobility (M/S)	5-25 m/s
Packet Inter-Arrival Time (S)	exponential(1)
Packet Size (Bits)	exponential(1024)
Transmit Power (W)	0.175
Data Rate (Mbps)	11Mbps
Mobility model	Random waypoint

Table 5.1 Bayesian Simulation Parameters

SIMULATION PARAMETERS	
Examined Protocols	DTM
Simulation Time	1000 seconds
Simulation Area(MxM)	1500x300
Number Of Nodes	30
Traffic Type	UDP
Performance Parameter	Average delay, Packet Delivery ration, Packet Energy, Packet overhead
Initial Energy (joules)	100 joules
Mobility (M/S)	5-25 m/s
Packet Inter-Arrival Time (S)	exponential(1)
Packet Size (Bits)	exponential(1024)
Transmit Power (W)	0.175
Data Rate (Mbps)	11Mbps
Mobility model	Random waypoint

Table 2.5 DTM Simulation Parameters

SIMULATION PARAMETERS	
Examined Protocols	DTM-ICN
Simulation Time	1000 seconds
Simulation Area(M×M)	1500x300
Number Of Nodes	32
Traffic Type	UDP
Performance Parameter	Average delay, Packet Delivery ration, Packet Energy, Packet overhead
Initial Energy (joules)	100 joules
Mobility(M/S)	5-25 m/s
Packet Inter-Arrival Time (S)	exponential(1)
Packet Size (Bits)	exponential(1024)
Transmit Power (W)	0.075
Data Rate (Mbps)	11Mbps
Mobility model	Random waypoint

Table 5.3 DTM-ICN Simulation Parameter

5.2 Comparative Analysis

we conduct a comparative analysis, contrasting our trust and security-based protocol operating under the best settings identified with Bayesian trust-based routing [12, 15], Dynamic trust and security management protocol without ICN architecture and with INC architecture. Bayesian trust-based routing relies on the use of trust information maintained by a Bayesian based trust management system (such as a Beta reputation system [12, 15]) to make routing decisions. In a Bayesian trust management system, the trust value is assessed using the Bayes estimator, updated by both direct observations and indirect recommendations. The direct observations are directly used to update the number of positive and negative observations, whereas the recommendations are discounted by the confidence [12] or belief [15] of the trustor toward the recommender. Under Bayesian trust-based routing, a node is chosen as the message carrier only if its trust value is in the top Ω percentile and higher than the message carrier trust threshold T_f.

Figure 2 compares the packet delivery ratio of Bayesian, DTM and DTM-ICN.The results demonstrate that our trust-based secure routing protocol designed to maximize delivery ratio, As compare to our protocol to Bayesian trust-based protocol and DTM protocols have less performance degradation in message delivery ratio.

Figure 3 compare the Packet Average delay of Bayesian, DTM and DTM-ICN.The results demonstrate that our trust-based secure routing protocol designed to minimize the Average delay, As compare to our protocol to Bayesian trust-based protocol and DTM protocols have less performance degradation Average delay.

Figure 4 compare the Packet Overhead of Bayesian, DTM and DTM-ICN.The results demonstrate that our trust-based secure routing protocol designed to minimize the packet overhead, As compare to Bayesian and DTM protocols.

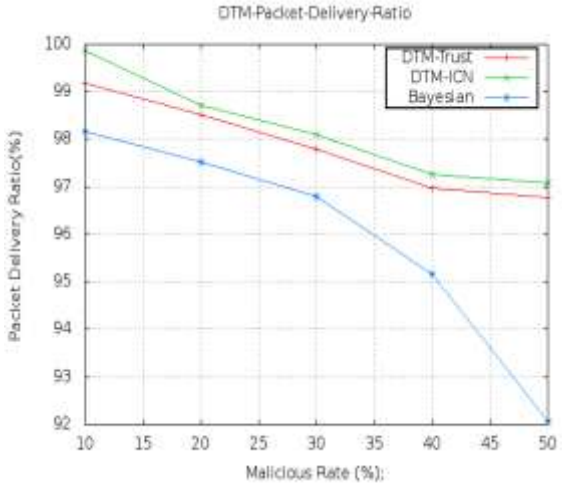

Figure 2 : Packet Delivery Ratio

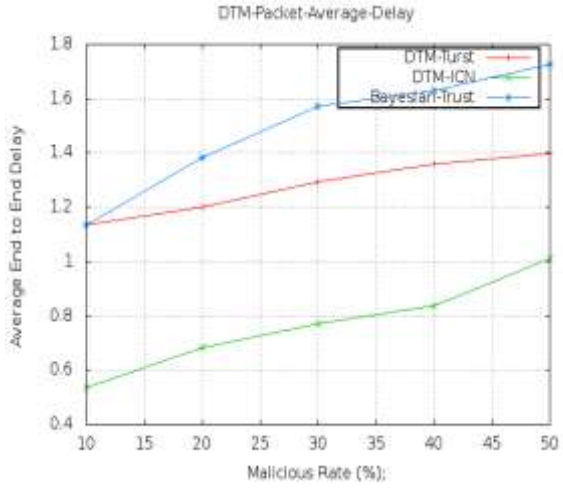

Figure 3: Packet Average Delay

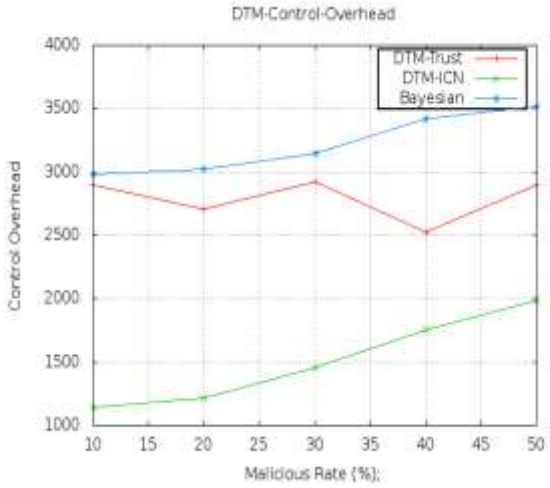

Figure 4: Packet Control Overhead

VI. CONCLUSION AND FUTURE WORK

In this paper, we designed and validated a trust and security management protocol using Information Centric-Network (ICN) architecture for DTNs and applied it to secure routing to demonstrate its utility. Our trust management protocol combines QoS trust with social trust to obtain a composite trust metric. We demonstrated how the results obtained at design time can facilitate dynamic trust management for DTN routing in response to dynamically changing conditions at runtime. We performed a comparative analysis of trust-based secure routing running on top of our trust management protocol with Bayesian trust-based routing and DTM routing in DTNs. Our results backed by simulation validation demonstrate that our trust-based secure routing protocol outperforms Bayesian trust-based routing. Our protocol approaches the ideal performance of epidemic routing in delivery ratio and message delay without incurring high message or protocol maintenance overhead.

There are several future research areas including (a) exploring other trust-based DTN applications with which we could further demonstrate the utility of our dynamic trust management protocol design; (b) designing trust management for DTNs considering social communities and performing comparative analysis with more recent works such as [2, 3].

REFERENCES

[1] "The ns-3 Network Simulator," Nov. 2011, http://www.nsnam.org/.

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

[3] E. Aivaloglou, and S. Gritzalis, "Hybrid Trust and Reputation Management for Sensor Networks," Wireless Networks, vol. 16, no. 5, July 2010, pp. 1493-1510.

[4] J. N. Al-Karaki, and A. E. Kamal, "Routing Rechniques in Wireless Sensor Networks: A Survey," IEEE Wireless Communications, vol. 11, no. 6, Dec. 2004, pp.6-28.

[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networks, vol. 54, no. 15, Oct. 2010, pp. 2787-2805.

[6] E. Ayday, H. Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay Tolerant Networks," Military Communications Conference, 2010, pp. 1788-1793.

[7] S. Braynov, and T. Sandholm, "Contracting with Uncertain Level of Trust,"Computational Intelligence, vol. 18, no. 4, 2002, pp. 501-514.

[8] J. Carbo, J. M. Molina, and J. Davila, "Trust Management Through Fuzzy Reputation," International Journal of Cooperative Information Systems, vol. 12, no. 1,2003, pp. 135-155.

[9] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-Tolerant Networking Architecture," RFC 4838, IETF, 2007.

[10] T. Chen, F. Wu, and S. Zhong, "FITS: A Finite-Time Reputation System for Cooperation in Wireless Ad Hoc Networks," IEEE Transactions on Computers, vol. 60, no. 7, July 2011, pp. 1045-1056.

[11] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges," Ad Hoc Networks, vol. 1, no. 1, 2003, pp. 12-64.

[12] M. K. Denko, T. Sun, and I. Woungang, "Trust Management in Ubiquitous Computing: A Bayesian Approach," Computer Communications, vol. 34, no. 3, 2011, pp. 398-406.

[13] T. E. Eugen Staab, "Tuning Evidence-Based Trust Models," International Conference on Computational Science and Engineering, Vancouver, Canada, August 2009, pp. 92-99.

[14] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks," ACM Transactions on Sensor Networks, vol. 4, no. 3, May 2008, pp. 1-37.

[15] A. Josang, and R. Ismail, "The Beta Reputation System," Bled Electronic Commerce Conference, Bled, Slovenia, June 17-19 2002, pp. 1-14.

[16] P. Resnick, and R. Zeckhauser, "Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System," Advances in Applied Microeconomics, vol. 11, no. 12, 2002, pp. 127-157.

[17] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, Feb. 2006, pp. 305-317.

[18] G. The odorakopoulos, and J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, Feb. 2006, pp. 318-328.

[19] C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A Formal Study of Trust-Based Routing in Wireless Ad Hoc Networks," IEEE Conference on Computer Communications, March 2010, pp. 1-9.

[20] K. Scott, S. Burleigh, "Bundle Protocol Specification", IETF FC 5050, experimen-tal, November 2007, http://www.ietf.org/rfc/rfc5050.txt.

[21] G. Xylomenos, B. Cici, Design and Evaluation of a Socket Emulator for Pub-lish/Subscribe Networks, Proc. of the Future Internet Symposium, 2010.

[22] J. H. Cho, A. Swami, and I. R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, 2011, pp. 562-583.

[23] J. D. Musa, "Operational Profiles in Software-Reliability Engineering," *IEEE Software*, vol. 10, no. 2, March 1993, pp. 14-32.

[24] I. Psaras, L. Wood, and R. Tafazolli, *Delay-/Disruption-Tolerant Networking: State of the Art and Future Challenges*, Dept. of El. Eng., University of Surrey, 2009.

[25] S. Trifunovic, F. Legendre, and C. Anastasiades, "Social Trust in Opportunistic Networks," *IEEE Conference on Computer Communications Workshops*, San Diego, CA, USA, March 2010, pp. 1-6.

[26] L. McNamara, C. Mascolo, and L. Capra, "Media Sharing Based on Colocation Prediction in Urban Transport," Proc. 14th Ann. Int'l Conf. Mobile Computing and Networking, 2008.

[27] P. Stuckmann and R. Zimmermann, "European research on future Internet design," IEEE Wireless Commun., vol. 16, no. 5, pp. 14–22, October 2009.

[28] J. Pan, S. Paul, and R. Jain, "A survey of the research on future Internet architectures," IEEE Commun. Mag., vol. 49, no. 7, pp. 26–36, July 2011.

[29] J. Choi, J. Han, E. Cho, T. Kwon, and Y. Choi, "Survey on content-oriented networking for efficient content delivery," IEEE Commun. Mag., vol. 49, no. 3, pp. 121–127, March 2011.

[30] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman,"A survey of information-centric networking," IEEE Commun. Mag., vol. 50, no. 7, pp. 26–36, July 2012