www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12698-12704

Dynamic Trust and Security Management Protocol For Delay Tolerant Networks using Information centric-Networks Architecture

Mrs. Suvarna L. kattimani, Mr. Jaeerahmad N. Indikar

Assistant Professor, Department of Computer Science and Engineering, B.L.D.E.A's Dr. P. G. Halakatti College of Engineering and Technology Bijapur-586103.
e-mail:suvarnaky1977@gmail.com

PG scholar, Department of Computer Science and Engineering, B.L.D.E.A's Dr. P. G. Halakatti College of Engineering and Technology Bijapur-586103.
e-mail:zaheer.indikar@gmail.com

Abstract—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. To avoid these anomalies we proposed Dynamic Trust and Security Management Protocol (DTSMP).In the current Internet architecture (IP-based architecture), data are treated as network elements as a series of bytes that have to be transferred from a specific source to a specific destination. But the network elements have no knowledge of the information they transfer a, hence cannot realize optimizations that would be possible (e.g., information replication at various points, information-aware traffic engineering, smart in-network caching). To overcome these issues we use the Information Centric-Networks (ICN) architecture for our proposed DTSM protocol. We design and validate the Dynamic Trust and Security Management protocol for delay tolerant networks (DTN) for better optimized secure routing in DTN environment; this includes well-behaved, selfish and malicious nodes. Proposed work is analyzed and validated via extensive simulation. Our protocol determine and apply the best optimized operational setting at the runtime in response to dynamically changing network environment, by will minimize the trust bias and maximize the routing performance. We do comparative analysis with other trust protocols like Bayesian trust-based protocol, DTSM protocol (proposed) with IP-based architecture and DTSMP protocol (with ICN architecture). The results demonstrate that DTSM protocol is able to deal with selfish behavior, malicious, and unreliable nodes. It also shows that our DTSM protocol work efficiently on INC architecture which improve the performance of our protocol. Furthermore proposed protocol can deal effectively with message overhead and message delay which will increase the significant gain in delivery ratio.

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 behaviours.

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 self-contained message forwarding applications and delay-tolerant, based on the information-centric networks (ICN) architecture.
4. We develop the Information Centric-Networks (ICN) Architecture in order to access information based on identifiers of the information instead of identifiers of the host addresses.
5. We perform comparative analysis of trust and security management protocol with respective the Bayesian trust-

based routing protocols and security management protocol using Information Centric-Networks (ICN) architecture.

II. RELATED WORK

A Credit Based Incentive System protocol

Encounter based routing is proposed and analyzed by Ing-Ray Chen [9]. They considered the quality-of-service (QoS) trust properties connectivity and social trust based properties honesty and unselfishness for trust evaluation in the routing protocol. In their literature they have reviewed two different protocols, an equal-weight QoS, social trust based management protocol and in this they have considered a QoS trust management protocol. A Credit Based Incentive System is proposed in [5], which allows the routing protocol to search the most efficient and optimized routes to transfer the data, with incentive considerations, hence give protection against behavior of purposely waste transfer and unfairly increased rewards of selfish nodes.

Credit Based strategy are collegial to forward the messages, the idea is to gets certain amount of credit as a reward which later can be explore for its own profit. Credit Based are generally of two types: Message Trade Model and Message Purse Model.. In Message Trade Model the sender message pay credits to receivers in each hop-by-hop transmission until the message reach to the destination, which finally pays credits for the message forwarding. In Message Purse Model source node pay credits to the intermediate nodes which are involve in forward the messages to the destination

SATS Routing

Mohamed Elsalih Mahmoud [6] proposed and analyzed A secure data forwarding scheme, they called it as SATS. The SATS also uses credits to measure the node's cooperation in forwarding other node's messages and to maintain a record of fairness. It assign specific trust value by a trust system to each node. To measure how actively node forward other's messages the node's trust value is used.. The nodes with high trust values are considered in data forwarding to avoid the attackers or miss behaving node that are not participating in routing process. The SATS forces nodes for cooperation to only earn trust but also maintain it at higher values. Multilayer credit based incentive technique is proposed by Haojin Zhu [7], The scheme has feature to operate in distribution manner to encourage forwarding cooperation among DTN nodes. Which also help defend various attacks without depending upon any specialized hardware. The performance and efficiency of proposed method is further increased by different optimization techniques by exploiting the unique characteristics of DTNs.

Trust Evaluation

Security concerns for delay-tolerant networks always difficult as it vary depending on the environment and application. Authentication and privacy are often critical and these security concerns often difficult to establish in a network without determined connectivity because the network block complicated cryptographic protocols which often prevent key exchange and moreover each device must identify other regularly visible devices.[8][9] the use of PKI schemes solutions have been modified from mobile ad hoc network and DTN security research, using distributed certificate authorities[10] . The solutions from the delay-tolerant research community include are as follows:

- To receive the information encrypted the public identifier [11] is used based on identity-based encryption.
- The use of tamper-evident tables with a gossiping protocol.

Epidemic Routing Protocol

Vahdat and Becker et al. (2000) published Epidemic routing algorithm, & flooding-based forwarding algorithm proposed by [8]. The main goals of Epidemic Routing are to: i)minimize message latency ii) minimize the total resources consumed in message delivery and iii) maximize message delivery rate . In DTNs routing scheme, when the node receiving a message, it forwards a copy of it to all other nodes it encounters. Thus, the copy of message is spread throughout the network by mobile nodes and finally all nodes will have same copy of data. Although there is no guarantees of delivery of data are provided. This algorithm does a best-effort approach to reach destination. Their unique identifiers are stored in node's buffer and message.

PROPHET Routing Protocol

Lindgren et al., (2003) developed the probabilistic routing protocol using history of encounter and transitivity (PROPHET) is a probabilistic routing protocol developed. The protocol assumption is that node's mobility is not a random but it is a more of repeating behavior. In the scheme, it is assumed that the mobile nodes are often tend to pass through some locations more than others, this indicate that passing through previously visited locations is highly probable. As a result, the nodes that which met each other in the past are more likely to meet in the future [9, 10]. Routing protocol PROPHET proposed for reduce the wastage of network resources in Epidemic routing and improve the delivery probability.

Information Centric-Networks architecture

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 Dynamic trust and security management protocol for a delay tolerant networks environment with no centralized trusted authority but using the Information Centric-Networks (ICN) Architecture where multiple server cache are implemented specifically for information exchange based on content-type. All nodes are communicated through multiple hops. Consider If a node encounters another node, say, node i encounter node j, they exchange encounter histories certified by encounter tickets [16] so as to prevent trust related attacks to DTN routing. We include socially selfish nodes and malicious nodes. A selfish node is nodes which act on its own interest and includes the interests to its friends, group, or communities. i.e. in order to save its energy or the resources it only forward the data to its socially tied nodes. To represent the social ties we consider a friendship matrix [18]. This will be achieved by keeping the friend list in its local storage from each node within the network. When node becomes selfish it will only forward messages when it is friend to source, intermediate carriers, or the destination node. While the good behaving node will forwards message regardless whether node is in its friend list or not. A malicious node aims to break or interrupt the basic DTN routing functionality, In addition to dropping packet, a malicious node can perform some of the following trust related attacks.

- **Self-promoting attacks:** In this kind of attack the node promote its importance by rendering good recommendations for itself so as to attract packets routing in order to drop the packets.
- **Bad-mouthing attacks:** In this kind of attack the malicious node or the collective malicious nodes ruin the reputation or trust of well behaved nodes by rendering bad recommendations against, the good nodes so as to decrease the chance of packets routing through good nodes.
- **Ballot stuffing:** In this kind of attack the misbehaving node can increase the reputation of bad nodes, by providing good recommendations for them. With this it increase the chance of packets routing through malicious nodes and being dropped.

An attacker can perform random attacks to DTN routing. We introduce a random attack probability P(rand) to reflect random attack behavior. And we assume that if P(rand) <1, the malicious attacker is a reckless attacker; and if P(rand) < 1 it is a random attacker. Attack can be collaborative attack i.e. the malicious nodes in a system boost the other malicious nodes in order to focus on particular victim within to system. The bad mouthing attack and ballot stuffing are the kind of collaborative attack where in bad mouthing the reputation of good node is ruined by giving the bad recommendations. As in ballot stuffing the bad node gives a good recommendation for the malicious nodes. To overcome with this attack we design application-level trust optimization with setting a recommender threshold T-rec to filter out inferior trustworthy recommenders and a trust carrier threshold T-f to select trustable carriers for message forwarding. Both the thresholds are dynamically changed in response to environment changes.

IV. DYNAMIC TRUST AND SECURITY MANAGEMENT PROTOCOL (DTSMP)

A. *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:

The capability of node to deliver messages or data to the destination in communication network is defined as QoS trust. To measure the QoS trust level of the node we consider "energy" and "energy". The energy QoS trust is about the energy of a node to perform preprocessing and the basic routing function. The connectivity QoS trust is defined as the ability of a node to communicate with other nodes due to its movement patterns.

Social trust:

Social trust is trust or the belief in social relationships and friendship in social ties or on honesty within the nodes. To measure the social trust level in node we consider social "unselfishness" and "healthiness". The unselfishness is nothing but the belief of social trust whether a node is socially selfish. Whereas the healthiness is the belief of social trust whether a node is malicious. In DTN routing, message delay and delivery ratio are two important factors. It consider "unselfishness", "healthiness" and "energy" in order to achieve high message delivery ratio, and we consider "connectivity" to achieve low message delay.

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.

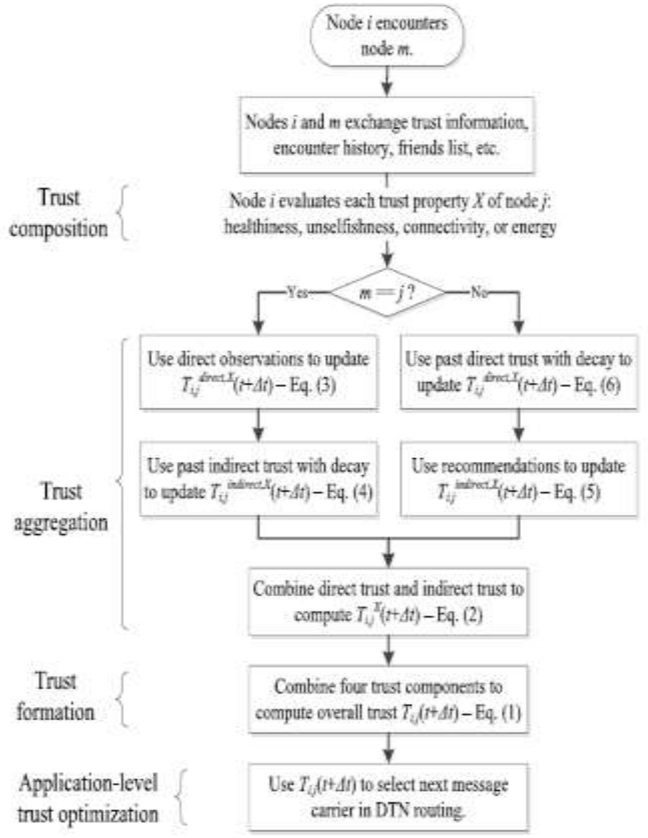

Node i encounters node m.
Nodes i and m exchange trust information, encounter history, friends list, etc.
Trust composition
Node i evaluates each trust property X of node j: healthiness, unselfishness, connectivity, or energy
$m = j$?
Yes
No
Use direct observations to update $T_{i,j}^{direct,X}(t+\Delta t)$ – Eq. (3)
Use past direct trust with decay to update $T_{i,j}^{direct,X}(t+\Delta t)$ – Eq. (6)
Trust aggregation
Use past indirect trust with decay to update $T_{i,j}^{indirect,X}(t+\Delta t)$ – Eq. (4)
Use recommendations to update $T_{i,j}^{indirect,X}(t+\Delta t)$ – Eq. (5)
Combine direct trust and indirect trust to compute $T_{i,j}^{X}(t+\Delta t)$ – Eq. (2)
Trust formation
Combine four trust components to compute overall trust $T_{i,j}(t+\Delta t)$ – Eq. (1)
Application-level trust optimization
Use $T_{i,j}(t+\Delta t)$ to select next message carrier in DTN routing.

Figure 1: A Flowchart for Trust Protocol Execution.

Trust Module

Node's trust level is defined as a real number in the range of [0, 1], with 0 indicating complete distrust, 0.5 ignorance, and 1 complete trust. We consider a trust formation design, 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:

$$T_{i,j}(t) = \sum_{X}^{all} w^{X} \times T_{i,j}^{X}(t) \qquad (1)$$

In (1),Where X represent the trust property, (X = healthiness, unselfishness, connectivity and energy), w^X is the weight associated with trust property X, and $T_{i,j}^{X}(t)$ is node *i*'s trust in trust property *X* toward node *j*

When evaluating trust value $T_{i,j}(t)$, we adopt some notations as follows:

- Node i is the trustor.

- Node j is the trustee.
- Node m is a newly encountered node.
- Node k is a recommender.

Node i (trustor) updates its trust toward node j (trustee) in trust property X upon encountering a node at time t over an encounter interval $[t, t + \Delta t]$ as follows:

$T_{i.j}^{X}(t + \Delta t) = \beta T_{i,j}^{direct,X}(t + \Delta t) + (1 - \beta) T_{i,j}^{indirect,X}(t + \Delta t)$ (2)

In (2), $T_{i,j}^{direct,X}(t + \Delta t)$ and $T_{i,j}^{indirect,X}(t + \Delta t)$ (4) are direct trust based on direct observation and indirect trust based on recommendation of node i towards node j in X at time $t + \Delta t$ respectively, and β in the range of [0, 1] is a parameter to weigh node i's own direct trust assessment toward node j. Every trust property X has its own specific β value under which subjective $T_{i.j}^{X}(t)$ obtained is accurate. Trust update is triggered by encountering events. On encounter of each event, node i obtains either direct observations toward j or indirect recommendations towards node j. this indicate decision making selection yes or no.

Trust Update upon Node i Encountering Node j

When node j encounter at time t, the node i updates direct trust $T_{i,j}^{direct,X}(t + \Delta t)$ (3), based on direct observation or with the past experience or by past interaction with node j at the interval$[t, t + \Delta t]$. If the monitoring node i unable to monitor properly node j because of encountering of nodes short contact time, it accommodate to this situation by discarding the current monitoring result and instead updating direct trust by its past direct trust toward j decayed over the time interval Δt to model trust decay over time interval. This ensure that the node i will update the direct trust $T_{i,j}^{direct,X}(t + \Delta t)$ (6) only if the node i directly encounter with node j at time t and it have all the information for property of X encounter at the time intervals. Otherwise the node j will update trust by it's past experience $T_{i,j}^{direct,X}(t + \Delta t)$ decayed $T_{i,j}^{direct,X}(t)$ over time Δt.

Application-Level Trust Optimization DTN Routing

When node i encounters node j, to reduce the message delay or to improve message delivery ratio it decide based on trust value whether or not node m can be the next message carrier. We use two parameters for application-level optimization routing performance maximization. First parameter described earlier the minimum trust threshold T-rec for the selection of recommenders. The high T-rec blocks bad-mouthing or ballot stuffing attacks also discourages recommendations, so "indirect trust" may be falling apart unnecessarily because of lack of recommendations. The low T-rec on the other hand encourages recommendations also opens door to malicious attacks. Second parameter is the minimum trust threshold T-f for the selection of the next message carrier. Our main aim is to identify the best application level trust optimization parameter settings in terms of T-rec and T-f to maximize the performance of the DTN routing.

B. DTSM-ICN

The design principles of DTSM-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.
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) protocol) or using native ICN for high speed optical links.

Information-centric network architectures, introduces three types of network entities consume, provide (producer) and relay (carrier) data in the network as shown in figure 2:

• **Consumers** request data by the network here in our case for example trust value of node. A consumer can be a source node, internal node, or destination nodes that access data in DTN from other node (e.g., Intermediate nodes). Consumer must know the name of the content in order to request for the data-content.

• **Producers** provide the data to the consumers here producers are nothing but the cache server or node which hold information about all other nodes within the network there can be more than two cache server can be implemented to increase the availability of information.

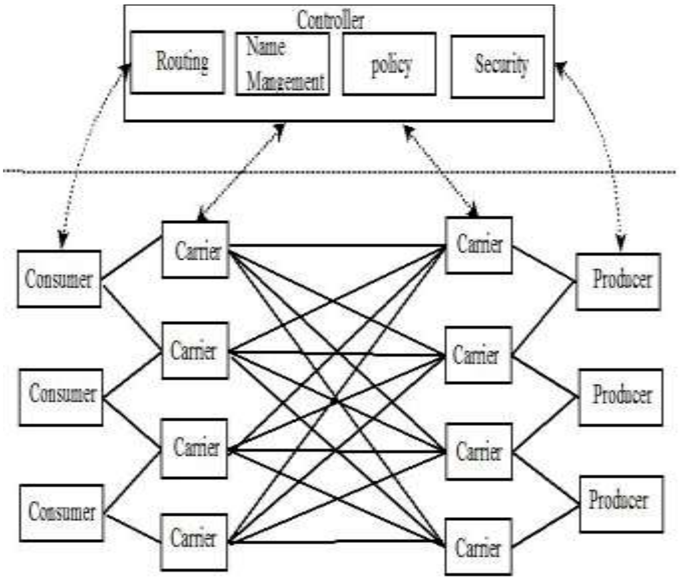


Figure 2: Information centric-networks architecture.

• **Carriers** are the nodes that deliver the request and response packets between the consumers and the producers as node are mobile in nature node location may change more often, and then it uses the intermediate nodes for request and response. Additionally, Carriers or intermediate nodes can cache the data contained within the response packets and even they can respond to requests made from the consumers on behalf of the producers.

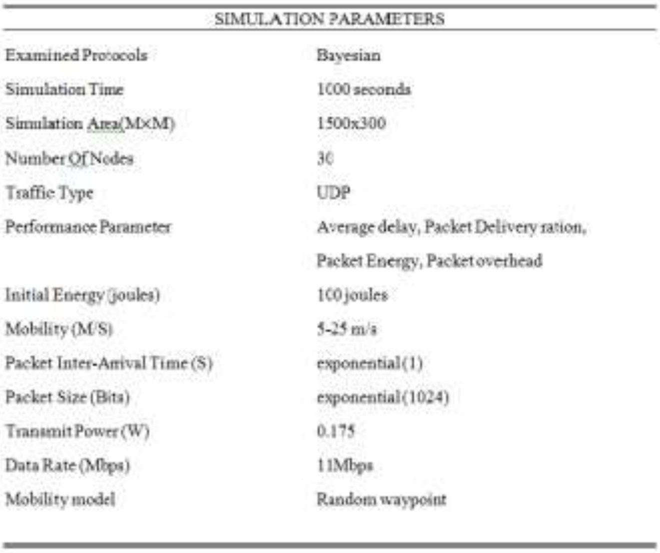
V. RESULTS

A. 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.

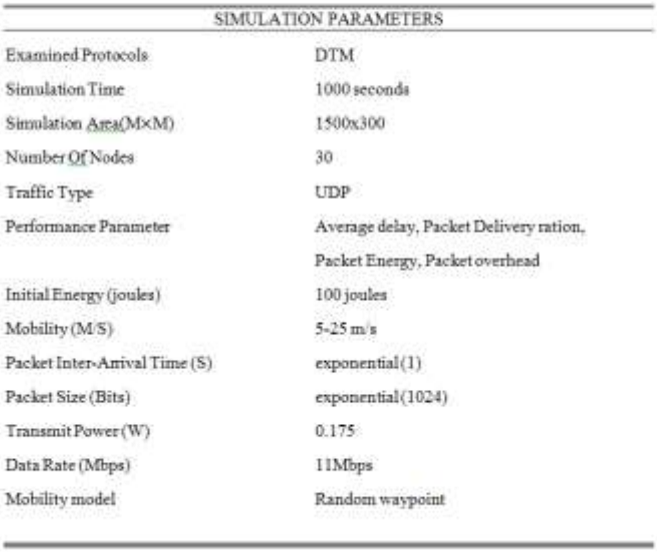
Bayesian Trust protocol: The simulation parameter for Bayesian is as shown in Table 1. A single scenario comprising of 30 mobile nodes moving at a variable speed from 5 meter per seconds to 25 meter per second. The number of node can be select explicitly and even the mobility (m/s) can be set explicitly, 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 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.



SIMULATION PARAMETERS	
Examined Protocols	Bayesian
Simulation Time	1000 seconds
Simulation Area(M×M)	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

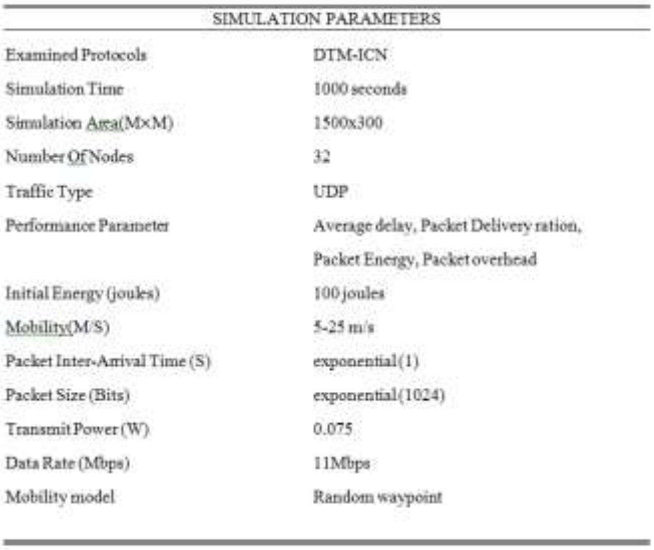
Table 1 Bayesian Simulation Parameters.



SIMULATION PARAMETERS	
Examined Protocols	DTM
Simulation Time	1000 seconds
Simulation Area(M×M)	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 DTM Simulation Parameters.

DTM-ICN: DTM Protocol: The simulation parameter for DTM-ICN is as shown in Table 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	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 3 DTM-ICN Simulation Parameter

B. *Comparative Analysis*

We conduct a comparative analysis, dissimilarity of 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. To make routing decision Bayesian trust-based routing depend on the trust information maintained by a Bayesian based trust management system (such as a Beta reputation system [12, 15]). Bayes estimator is use to access the trust value in a Bayesian trust management system. The trust value can be updated by both indirect recommendations and direct observations. The recommendations are considered by the confidence [12] or belief [15] of the trustor toward the recommender, whereas direct observations are directly used to update the number of positive and negative observations. A node is chosen as message carrier only if top Ω and its message carrier trust threshold T_f in Bayesian trust-based routing.

Figure 3 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.

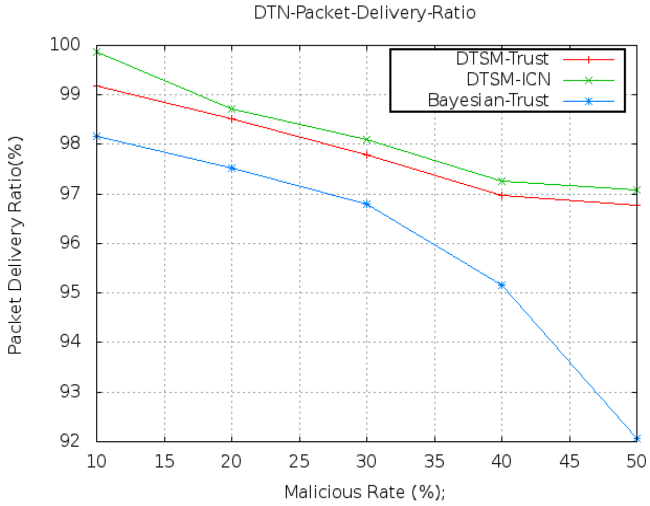


Figure 3 : Packet delivery Ratio.

Figure 4 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.

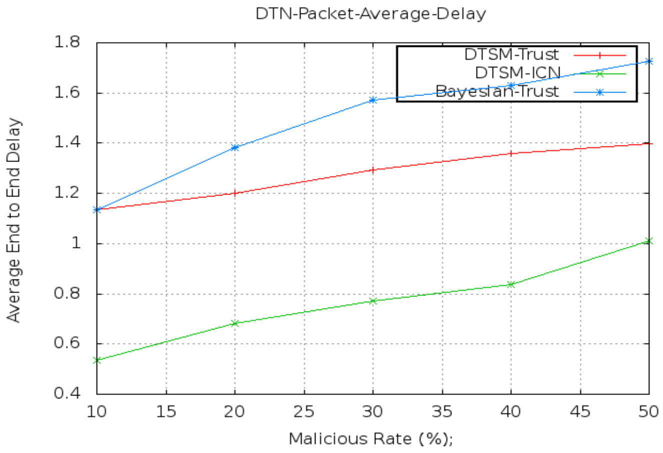


Figure 4: Packet Average Delay.

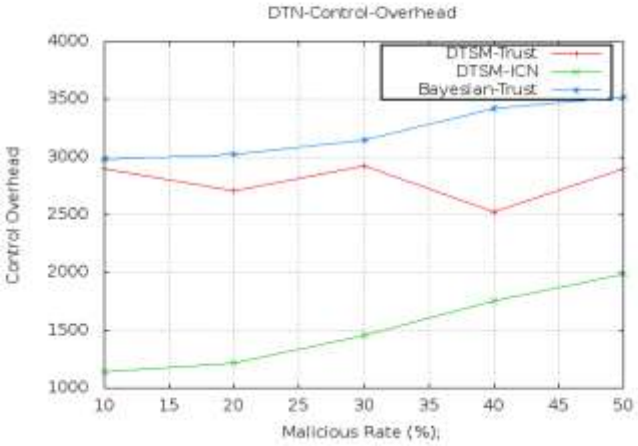


Figure 5: Packet Control Overhead.

Figure 5 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.

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 delay tolerant networks, and applied it to secure routing to demonstrate its utility. Our trust and security management protocol combines both QoS trust with social trust to obtain a combined trust metric. We demonstrate how the results obtained at design time can alleviate dynamic trust and security management for DTN routing in response to dynamically changing DTN environment at runtime. We performed a comparative analysis of trust and security based routing running on top of our trust and security management protocol with Bayesian trust-based routing and DTSM routing in DTNs. Our results demonstrate that our dynamic trust and security management protocol outperforms Bayesian trust-based routing and we show that the implementing ICN architecture to the DTSMP, improves the efficiency of the DTN. Our protocol approaches the ideal performance of routing in delivery ratio and average message delay without getting high message or protocol maintenance overhead.

There are several future scope for the research areas including (a) Designing trust and security management for DTNs considering social communities and performing comparative analysis with more recent works such as [2, 3]. (b) Improving the efficiency of ICN architecture by overcoming the drawback of mapping of names for large information. (c) Exploring other trust-based DTN applications with which we could further demonstrates the utility of our dynamic trust and security management protocol design.

REFERENCES

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

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

[3] I.R. Chen, F. Bao, M. Chang, and J.H. Cho, "Supplemental Material for 'Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing'," IEEE Trans. Parallel and Distributed Systems, 2013.

[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] I.R. Chen and T.H. Hsi, "Performance Analysis of Admission Control Algorithms Based on Reward Optimization for Real-Time Multimedia Servers," Performance Evaluation, vol. 33, no. 2, pp. 89-112, 1998.

[7] S.T. Cheng, C.M. Chen, and I.R. Chen, "Dynamic Quota-Based Admission Control with Sub-Rating in Multimedia Servers," Multimedia Systems, vol. 8, no. 2, pp. 83-91, 2000.

[8] S.T. Cheng, C.M. Chen, and I.R. Chen, "Performance Evaluation of an Admission Control Algorithm: Dynamic Threshold with Negotiation," Performance Evaluation, vol. 52, no. 1, pp. 1-13, 2003.

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

[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. Theodorakopoulos, 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