INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A NOVEL APPROACH FOR SECURED ROUTING BY TRUST MANAGEMENT IN DELAY TOLERANT NETWORKS

Ms.P.Pappathi[#1],Ms.S.B. Suganya[#2],Ms.S. Banumathi[#3] Mr.J Joe Paul[*4]

[#]Students,[*]Assistant Professor
Department of Applied Electronics and Department of Computerscience
Chandy college of engineering
Tutucorin(T.N) India

[1]pappathi91@gmail.com [3]banumathi592@gmail.com [4]jeanvilavan@gmail.com

Abstract: - The main objective of this paper is design and validates a dynamic trust management protocol for secure routing optimization in DTN environments in the presence of well-behaved, selfish and malicious nodes. Delay/Disruption Tolerant Networks (DTNs) have been identified as one of the key areas in the field of wireless communication. DTNs are characterized by large end-to-end communication latency and the lack of end-to-end path from a source to its destination. These characteristics pose several challenges to the security of DTNs. In this paper, to design and validate a dynamic trust management protocol for secure routing optimization in DTN environments in the presence of well-behaved, selfish and malicious nodes. A novel model based methodology for the analysis of our trust protocol and validates it via extensive simulation. To perform a comparative analysis of our proposed routing protocol against Bayesian trust-based and non-trust based (PROPHET and epidemic) routing protocols. Our trust based routing protocol can effectively trade off message overhead and message delay for a significant gain in delivery ratio**.**

I. INTRODUCTION

Delay-tolerant networking is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space. Security mechanism for DTNs which enables us to detect misbehaviour due to Byzantine adversaries. Security is essential to communication between entities in the internet. Delay tolerant and disconnected Mobile Ad Hoc Networks (MANET) are a class of networks characterized by high end-to-end path latency and frequent end-to-end disconnections and are often termed as challenged networks. In these networks nodes are sparsely populated and without the existence of a central server, acquiring global information is difficult and impractical if not impossible and therefore traditional security schemes proposed for MANETs cannot be applied. DTNs are highly applicable for sensor-based networks, terrestrial wireless networks, satellite networks, underwater acoustic networks. Security concerns for delay-tolerant networks vary depending on the environment and application, though authentication and privacy are often critical. These security guarantees are difficult to establish in a network without persistent connectivity because the network hinders complicated cryptographic protocols, hinders key exchange, and each device must identify other intermittently visible devices. The ability to transport, or route, data from a source to a destination is a fundamental ability all communication networks must have. Delay and disruption-tolerant networks (DTNs), are characterized by their lack of connectivity, resulting in a lack of instantaneous end-to-end paths.

In these challenging environments, popular ad hoc routing protocols such as AODV and DSR fail to establish routes. This is due to these protocols trying to first establish a complete route and then, after the route has been established, forward the actual data. However, when instantaneous end-to-end paths are difficult or impossible to establish, routing protocols must take to a "store and forward" approach, where data is incrementally moved and stored throughout the network in hopes that it will eventually reach its destination. A common technique used to maximize the probability of a message being successfully transferred is to replicate many copies of the message in the hope that one will succeed in reaching its destination. This is feasible only on networks with large amounts of local storage and inters node bandwidth relative to the expected traffic.

In many common problem spaces, this inefficiency is outweighed by the increased efficiency and shortened delivery times made possible by taking maximum advantage of available unscheduled forwarding opportunities. In others, where available storage and inter node throughput opportunities are more tightly constrained, a more discriminate algorithm is required.A DTN is a network of smaller networks. It is an overlay on top of special-purpose networks, including the Internet. DTNs support interoperability of other networks by accommodating long disruptions and delays between and within those networks, and by translating between the communication protocols of those networks. In providing these functions, DTNs accommodate the mobility and limited power of evolving wireless communication devices.

DTNs were originally developed for interplanetary use, where the speed of light can seem slow and delay-tolerance is the greatest need. However, DTNs may have far more diverse applications on Earth, where disruption-tolerance is the greatest need. The potential Earth applications span a broad range of commercial, scientific, military, and public-service applications. DTNs can accommodate many kinds of wireless technologies, including radio frequency (RF), ultra-wide band (UWB), free-space optical, and acoustic (sonar or ultrasonic) technologies.Trust management forms the basis for communicating policy among system elements and demands credential checking for access to all virtual private service resources—along with careful evaluation of credentials against specified policies—before a party can be trusted.Trust management is an abstract system that processes symbolic representations of social trust, usually to aid automated decision-making process. Such representations, e.g. in a form of cryptographic credentials, can link the abstract system of trust management with results of trust assessment. Trust management is popular in implementing information security, specifically access control policies. The concept of trust management has been introduced by Blaze to aid the automated verification of actions against security policies. In this concept, actions are allowed if they demonstrate sufficient credentials, irrespective of their actual identity, separating symbolic representation of trust from the actual person. Trust management techniques to specify dynamic policies in complex integrated service-oriented networks.

A) Advantages of Trust Management:

1. Trust management provides the basis for communicating policy among system elements.
2. There is no unified policy-based mechanism through which to scalably handle access control, intrusion detection, and other recovery mechanisms consistently across a large distributed system.
3. Trust management provides a unified approach to specifying and interpreting security policies, credentials, and relationships.

B) Discussion on Trust/Reputation models

The most relevant sources of information considered by the trust and reputation models presented before, are direct experiences and witness information. In e-markets, sociological information is almost non-existent and, in order to increase the efficiency of actual trust and reputation models, it should be considered. However, there is no reason to increase the complexity of models introducing trust evidence if, later, they have to be used in an environment where it is not possible to realize their capabilities. The aggregation of more trust and reputation evidence is useful in a computational model but it can increase its complexity making a general solution difficult. Several models are dependent on the characteristics of the environment and a possible solution could be the use of adaptive mechanisms that can modify how to combine different sources of information in a given environment. A lot of trust and reputation definitions have been presented and there are several works that give meaning to both concepts. There is a relation between both the concepts that should be considered in depth: reputation is a concept that helps to build trust on others. Nowadays, game theory is the predominant paradigm considered to design computational trust and reputation models. In all likelihood, this theory is taken into account because a significant number of economists and computer scientists, with a strong background in game theory and artificial intelligence techniques, are working in multi-agent and e-commerce contexts. Game theoretical models produce good results but, when the complexity of the agents, in terms of social relations and interaction increases, become too restrictive. The exploration of new possibilities should be considered and, for example, there should be a merging of cognitive approaches with game theoretical ones. Apart from that, more trust evidence should be considered, as well as time-sensitive trust metrics. Represent the first step to encourage the improvement of computational trust. An important issue in modeling trust is represented by the transferability of trust judgments by different agents. Social scientists agree to consider unqualified trust values as not transferable, but a more pragmatic approach would conclude that qualified trust judgments are worth being transferred as far as decisions taken considering others' opinion are better than the ones taken in isolation. In [24] the authors investigated the problem of trust transferability in open distributed environments, proposing a translation mechanism able to make information exchanged from one agent to another more accurate and useful.

II. SYSTEM DESIGN AND MODULES

Our trust protocol considers trust composition, trust aggregation, trust formation and application-level trust optimization designs.First two nodes(i,m) are encountered and exchange the trust information. Node i evaluates the trust property of node j. The m and j nodes are equal then use direct observation and past indirect trust with decay to updation. Otherwise use past direct trust with decay and recommendation updation. Combine this trust components and select the next message in DTN routing.

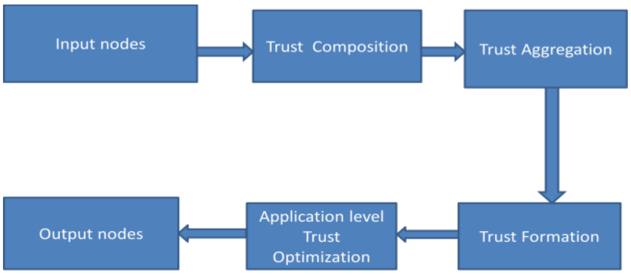


Figure.1.Block diagram of Dynamic Trust Management

A) Trust Composition

Consider the two nodes i , m. The node i encounters the node m. The i and m nodes are exchange the trust information, encounter history, friends list etc. The node i evaluates each trust property X of node j healthiness, unselfishness, connectivity and energy. The trust composition has two properties.

B) QoS trust

To 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.

C) Social trust

To 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, and consider friendship as a major factor for determining a node's socially selfish behaviour.

To evaluate the trust property X as follows:

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

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.

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

D) Trust Aggregation

When a monitoring node (node i) cannot properly monitor a trustee node (node j) upon encounter because of a short contact time, it adapts 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.

Node i's trust in X toward node j at time t+Δt upon encounter at time t, is calculated by:

$$T_{i,j}^{direct,X}(t+\Delta t) = \begin{cases} T_{i,j}^{encounter,X}(t+\Delta t), & if\ C_{i,j}^{direct,X}(t) = true \\ e^{-\lambda_d \Delta t} \times T_{i,j}^{direct,X}(t), & if\ C_{i,j}^{direct,X}(t) = false. \end{cases}$$

In this case, since there is no new "indirect trust," node i simply updates with its past experience decayed over Δt,

$$T_{i,j}^{indirect,X}(t+\Delta t) = e^{-\lambda_d \Delta t} \times T_{i,j}^{indirect,X}(t).$$

When node i encounters node m, m≠j then node i uses its 1-hop neighbors (including node m) as recommenders to update "indirect trust". In this case, node i weighs node k's recommendation with node i's referral trust toward node k.

$$T_{i,j}^{indirect,X}(t+\Delta t) = \begin{cases} e^{-\lambda_d \Delta t} \times T_{i,j}^{indirect,X}(t), & if\ |R_i| = 0, \\ \frac{\sum_{k \in R_i} \{T_{i,k}^{X}(t) \times T_{k,j}^{X}(t)\}}{\sum_{k \in R_i} T_{i,k}^{X}(t)}, & if\ |R_i| > 0. \end{cases}$$

In this case, since there is no new "direct trust," node i simply updates with its past experience decayed over Δt,

$$T_{i,j}^{direct,\quad X}(t+\Delta t) = e^{-\lambda_d \Delta t} \times T_{i,j}^{direct,X}(t).$$

E) Trust Formation

Trust formation means to form the trust for the above trust aggregation. Two types are used to form the trust.

1. To combine the above direct and indirect trust and compute the trust property.

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

2. To combine four trust components and compute the overall trust

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

F) Application Level Trust Optimization

When node i encounters node j, it uses T_i; j(t) to decide whether or not node m can be the next message carrier to shorten message delay or improve message delivery ratio.To use two application-level optimization parameters for encounter-based DTN routing performance maximization. One parameter is the minimum trust threshold T_{rec} for the selection of recommenders. A high T_{rec} blocks bad-mouthing or ballot stuffing attacks but discourages recommendations, so "indirect trust" may be decayed unnecessarily because of lack of recommendations. A low T_{rec} on the other hand encourages recommendations but opens door to malicious attacks. Another application-level optimization parameter is the minimum trust threshold T_f for the selection of the next message carrier.

III. PERFORMANCE EVALUATION AND COMPARATIVE STUDY

To evaluate the performance of the method, the developed system is compared with various performance metrics. The performance metrics are like delivery ratio, message delay and message overhead. The performance metrics can be calculated as follows,

Table 1. Comparison of Delivery Ratio with Various methods

Methods	Bayesian	Prophet	Trust-Traceable	Epidemic
0%	52	45	42	30
5%	50	45	42	30
10%	49	45	42	31
15%	48	44	41	31
20%	47	43	40	32
25%	46	42	39	32
30%	45	42	39	33
35%	44	41	38	33
40%	43	41	38	34
45%	42	40	37	34
50%	40	40	37	35

a. *Delivery Ratio*

The ratio of the number of delivered data packet to the destination is known as packet delivery ratio. This illustrates the level of delivered data to the destination

$$Packet\ Delivery\ Ratio = \frac{\sum Number\ of\ Packet\ Received}{\sum Number\ of\ Packet\ Send}$$

b. *Message Delay*

The average time taken by a data packet to arrive in the destination is known as end to end delay. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

$$Message\ Delay = \frac{\sum(Arrive\ Time - Send\ Time)}{\sum Number\ of\ Connections}$$

c. *Message Overhead*

In computer science, the routing overhead is any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to attain a particular goal. It can also be calculated as the difference between the actual or fixed values and the absorbed values.

$$Message\ Overhead = \frac{Actual\ Values}{Absorbed\ Values}$$

A) Comparative Study:

To analysis the performance of the developed system, it is compared with various performance metrics. This is shown in the below tables.

Table 2. Comparison of Message Delay with Various methods

Methods	Bayesian	Prophet	Trust-Traceable	Epidemic
0%	0.65	0.78	0.84	0.98
5%	0.65	0.78	0.84	0.98
10%	0.64	0.77	0.83	0.97
15%	0.64	0.77	0.83	0.96
20%	0.63	0.76	0.82	0.95
25%	0.63	0.76	0.82	0.94
30%	0.62	0.75	0.81	0.94
35%	0.62	0.75	0.81	0.93
40%	0.61	0.74	0.80	0.93
45%	0.61	0.74	0.80	0.92
50%	0.60	0.73	0.79	0.91

Table 3. Comparison of Message Overhead with Various methods

Methods	Bayesian	Prophet	Trust-Traceable	Epidemic
0%	10.5	5.6	4.7	3.5
5%	10.6	5.5	4.7	3.5
10%	10.7	5.4	4.7	3.5
15%	10.8	5.3	4.8	3.6
20%	10.9	5.2	4.8	3.6
25%	10.8	5.1	4.8	3.6
30%	10.7	5.0	4.8	3.6
35%	10.6	4.9	4.7	3.5
40%	10.5	4.8	4.7	3.5
45%	10.4	4.7	4.7	3.5
50%	10.3	4.6	4.6	3.4

To know the working of the developed system, it is compared with different methods. The comparison with different methods is shown below.

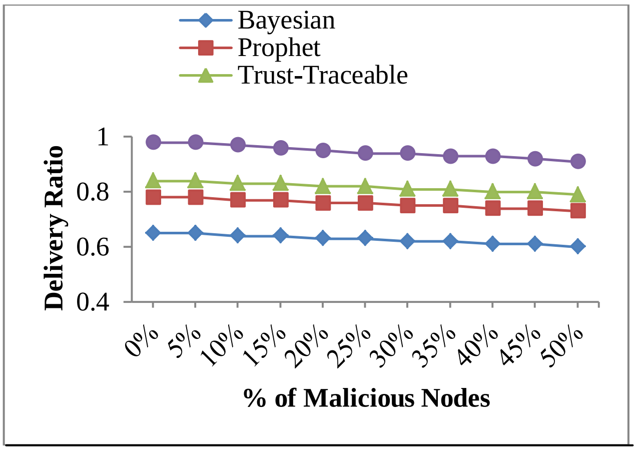


Fig. 2 Comparison of Delivery Ratio with Various methods

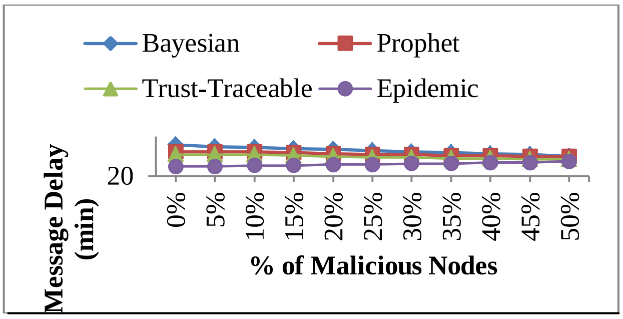


Fig. 3. Comparison of Message Delay with Various methods

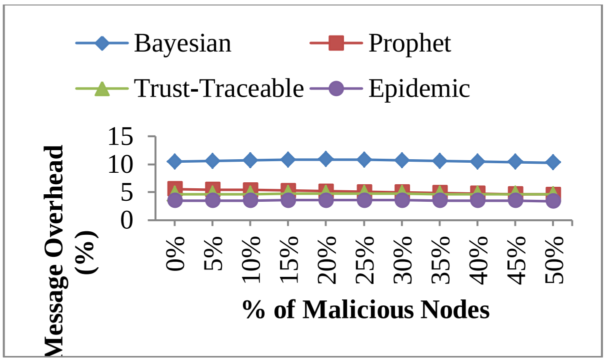
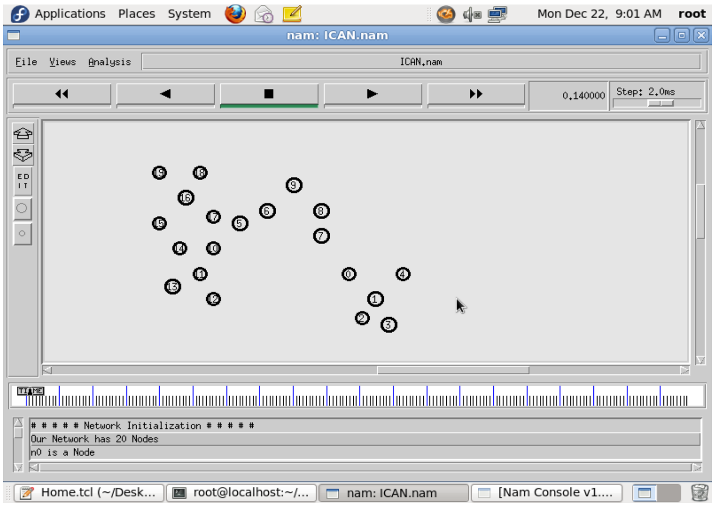


Fig. 4. Comparison of Message Overhead with Various methods

The above tables and figure shows the performance of the developed system which is compared with the methods, with the performance metrics of delivery ratio, message delay and message overhead.

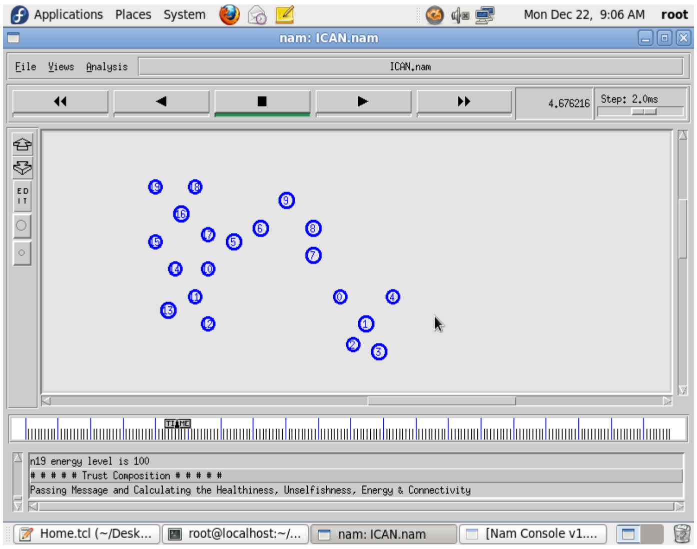
IV Simulation Result

In this process first the input nodes are selected and trust is composed. Selection of proper source and destination is made to transfer the message. Then the trust is formed .After the formation of the trust best routing path is find which avoid the delay of message transfer.



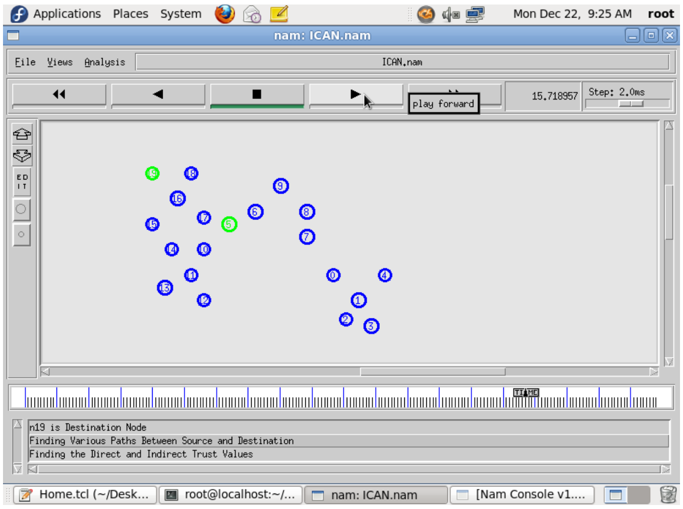
```
# # # # # Network Initialization # # # # #
Our Network has 20 Nodes
n0 is a Node
```

Figure. 5 Input nodes



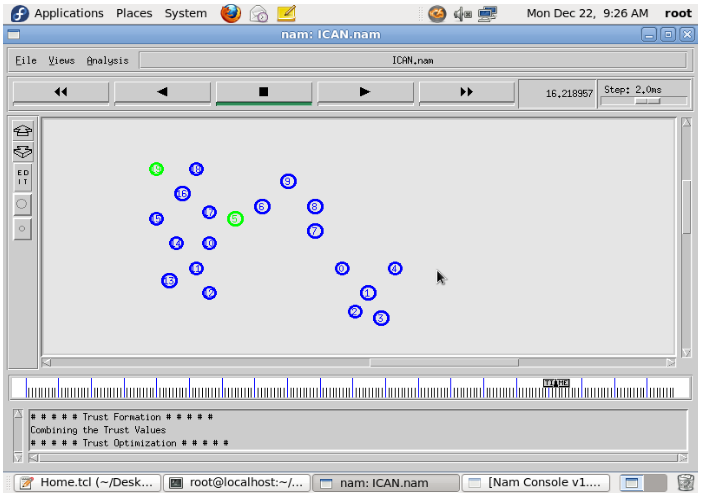
```
n19 energy level is 100
# # # # # Trust Composition # # # # #
Passing Message and Calculating the Healthiness, Unselfishness, Energy & Connectivity
```

Figure. 6 Trust composition



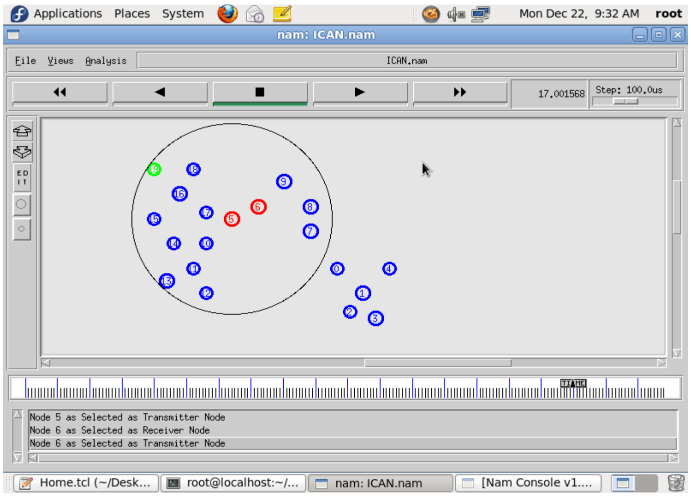
```
n19 is Destination Node
Finding Various Paths Between Source and Destination
Finding the Direct and Indirect Trust Values
```

Figure. 7 Selection of source and destination node



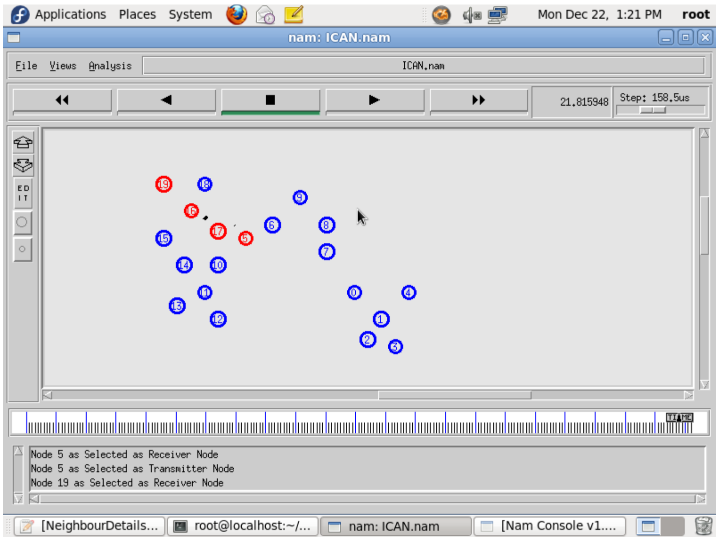
```
# # # # # Trust Formation # # # # #
Combining the Trust Values
# # # # # Trust Optimization # # # # #
```

Figure. 8 Trust Formation



```
Node 5 as Selected as Transmitter Node
Node 6 as Selected as Receiver Node
Node 6 as Selected as Transmitter Node
```

Figure. 9 Finding the best route



```
Node 5 as Selected as Receiver Node
Node 5 as Selected as Transmitter Node
Node 19 as Selected as Receiver Node
```

Figure. 10 Message Received

V CONCLUSION

In this paper, a dynamic trust management protocol for securing the routing optimization in DTN environment is used. First the nodes are gathered from the networks as input nodes. From the input nodes, the trust composition is established. Then the aggregation and the formation of trust are applied. Finally, the trust level is optimized to the application level. From the performance metrics and the experimental results, the method used in the paper shows better results than the other methods, which is used to compare with the method used in the paper.we designed and validated a trust management protocol 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. Our design allows the best trust setting for trust aggregation to be identified so that subjective trust is closest to objective trust for each individual trust property for minimizing trust bias. Further, our design also allows the best trust formation and application- level trust settings to be identified to maximize application performance. 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 non-trust-based routing protocols (PROPHET and epidemic) in DTNs. Our results backed by simulation validation demonstrate that our trust-based secure routing protocol outperforms Bayesian trust-based routing and PROPHET. Further, it approaches the ideal performance of epidemic routing in delivery ratio and message delay without incurring high message or protocol maintenance overhead.

REFERENCES

[1] Erman Ayday,Hanseung Lee and Faramarz Fekri "Trust Management and Adversary Detection for Delay Tolerant Networks"

[2] Haodong Wang, Bo Sheng, Chiu C. Tan, Qun Li (2008) "Comparing Symmetric-key and Public-key based Security Schemes in Sensor Networks: A Case Study of User Access Control" Proc. IEEE 28th Int'l Conf. Distributed Computing System (ICDCS), pp.11-18.

[3] Pointcheval. D and Stern. J, (1996) "Security Proofs for Signature Schemes," Proc. Advances in Cryptology (EUROCRYPT), pp. 387- 398.

[4] Pointcheval. D and Stern. J, (2000) "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 950, pp.182-193.

[5] Rivest. R, Shamir and Adleman. L (1978) "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol.21, no. 2, pp. 120-126.

[6] Ramesh kumar. M, Suresh Gnana Dhass. C (2012) "A Security of Wireless Sensor Networks and Analysis on Efficient Broadcast Authentication" International Journal of Advanced Research in Computer Science and Software Engineering.

[7] Ramesh kumar. M, Suresh Gnana Dhass. C (2012) "Design an Enhanced Certificate Based Authentication Protocol for Wireless Sensor Networks" International Journal of Advanced Research in Computer Science and Software Engineering.

[8] Swati Verma1, and Birendra Kumar Sharma (2011) "A New Digital Signature Scheme Based on Two Hard Problems" Int. J. Pure Appl. Sci. Technol., International Journal of Pure and Applied Sciences and Technology.

[9] Victor. R, Shen. L, Yu Fang Chung, Tzer Shyong Chen and Yu An Lin (2011) "A Blind Signature Based On Discrete Logarithm Problem" International Journal of Innovative Computing.

[10] Zhang. W, Subramanian. N and Wang. G (2008) "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM.