ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

*Volume 3, Special Issue 3, March 2014*

**2014 International Conference on Innovations in Engineering and Technology (ICIET'14)**
**On 21st & 22nd March Organized by**

**K.L.N. College of Engineering, Madurai, Tamil Nadu, India**

# Reputation Based Trust Management for Wireless Sensor Networks and Its Application to Secure Routing

[1#]R.Mohan Kumar, [2#] K.S.Ajitha, [3#]A.V.Ramprasad

Department of Electronics and Communication and Engineering, KLN College of Engineering, Sivagangai, Tamil Nadu, India.

Department of Electronics and Communication and Engineering, KLN College of Engineering, Sivagangai, Tamil Nadu, India

Department of Electronics and Communication and Engineering, KLN College of Engineering, Sivagangai, Tamil Nadu, India

**ABSTRACT—** Using delay tolerant networks it can be characterized by high-end-to-end latency to secure routing .It consist of frequent disconnection and communication over a unreliable wireless links .The methods used for the protocol to validate extensive simulation, and also the design and validation of dynamic trust management protocols for mobile networks .The application used to optimize and gain the quality of service. It is based on trust-based (Bayesian) and non-trust based (ProPHET and Epidemic).When we compare the both protocols the non-trust based provides high incurring message of trusted nodes with gives message delivery ratio. The parameter occurred as healthiness, unslefiness, connectivity and energy. The outperforms deals with the selfish behavior and is resilient against trust related attacks.

**KEYWORDS:** Trustworthiness, Social Trust, QOS Trust, Delay Tolerant network**.**

## I. INTRODUCTION

A challenge is to trust management protocol design in mobile networks is very exhibit a wide range of heterogeneous QoS characteristics are energy level ,bandwidth, moving speed etc., social behaviors consist of selfiness, honest, social connection etc., for sensing cable device are Carried by Smartphone and digital personal assistants. It's based on performance and security requirements in a dtn are socially selfish to outsiders and unselfish to friends. The operation built on the dtn is trust based routing protocol and to validate a dynamic trust management to optimize the population of misbehaving nodes. The combination of social trust deriving from social networks and quality of service it provide communication network into composite trust metric node in a DTN. We consider the healthiness and unselfishness of two social metrics, the notation of subjective trust Vs objective trust based on ground truth of protocol. The combination of social trust from social networks and the traditional quality has a composite trust metrics to assess the trust nodes. The application of trust reputation method referred to ITRM which can decode to low density parity check codes. Trust management and malicious node detection provides high data availability and packet delivery ratio with low latency in the presence of attackers called Byzantine. The maximization of dynamic trust management by adjusting formation of protocols.

Energy maintained for friend list and computed towards matching operations when there is no change in friend list. DTN communicate through energy, the comparison of Bayesian and PROPHET routing protocol which can act as epidemic routing protocol. It is another form of dynamically changing environment in mobile network variables with each density nodes, such as number of misbehaving nodes.

1. It is characterized into three levels: Node Dynamic, locality Dynamic and Network Dynamics. Network status can given by network topology, mobility pattern, population size. The application performance maximize the lifetime of throughput protocol design. The application

performance is to maximize the trust management protocols in response to changing DTN routing performance. Integration of trust and security metrics is routing and replication decision DTNs.

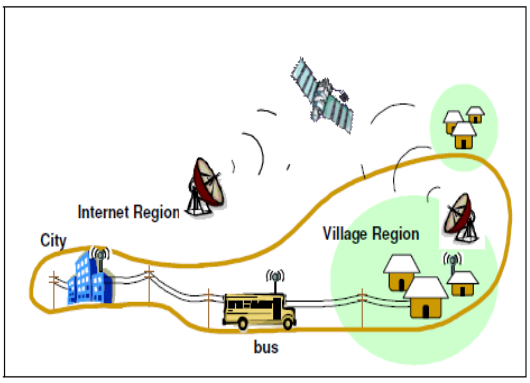


Fig 1: DTN Network

2. The utilization of model based stochastic petrinet techniques.The simulation yields actual ground truth nodes obtain from executing the trust protocol in response to dynamic changing network.

3. The outperformance Bayesian trust based protocol, in delivery ratio the epidemic routing which incurring high message or protocol maintenance overhead.

## II. RELATED WORK

In dynamic trust management used to perform design analysis to secure routing in direct and indirect method. The investigation of dynamic trust management by a trust based protocol may dynamically adjust the trust parameter in threshold condition in response with changing network environment dynamically in [1]. In proposed a novel based analysis method by which subjective trust with objective trust generated by actual network status. The utility of trust management protocol includes misbehaving node detection, trust based survivability management in dynamic trust management protocol design. Optimization of trust composition and trust formation for secure routing in mobile networks, delivery ratio are most important performance metrics for reducing delay and honesty. The investigation of dynamic trust management is built up on the parameter in response to changing the network dynamically. Definition of internet connection oriented service depends up on bidirectional connection between source and destination. Acknowledgement of receiving packets relatively loss of data in each link. In delay tolerant network presence of well behaved selfish and malicious node in [2], validate the dynamic trust management to determine trust bias and maximize the routing performance. The comparative analysis of routing protocol against Bayesian trust based and non trust based (PROPHET and epidemic). Its deal with selfish behaviours and resilient trusted attacks. The outperformance of Bayesian trust and PROPHET deal with epidemic routing in delivery ratio and message delay without incurring high message in [2, 3].

DTNs have attracted much attention in the networking research community, Most of DTNs are deployed in extreme environments (e.g., battlefields and developing regions), where the end-to-end connection which is the fundamental assumption of the Internet cannot be guaranteed. protocols designed for the Internet may not be applicable to DTNs. DTN characteristics and application requirements, in [3] suggests a top-down approach for DTN-protocol design to consider application priorities. In this focus on trust management and secure routing in DTNs.

A limitation of work is that consideration is given to inside attackers. Designed an iterative trust management scheme for DTNs is used discrepancies of indirect recommendations for adversary detection and used authentication as the underlying mechanism to evaluate a node in [3]. A node exchanges its trust evaluation with others and interactively updates its trust evaluation. Inconsistent trust evaluations are identified and removed iteratively until the trust evaluation converges in [3, 4].

Epidemic Routing in [5] provides message delivery in disconnected environments where no assumptions are made with regard to control over node movements or knowledge of the network's topology. Each host maintains a buffer containing messages, upon the two nodes exchange vectors to determine each messages held by the other. They initiate a transfer of new messages. The way messages are propagated throughout the network. Method used to delivery if a route is available but is expensive in terms of resources when the network is essentially flooded. The number of copies of the message is explored in [5, 6] Ni et al take a approach to reduce the overhead of flooding by only forwarding a copy with some probability $p < 1$, which is essentially randomized flooding. The Spray-and-Wait solution presented by Spyropoulos et al assigns a replication number of message and distributes message copies to a number carrying nodes and then waits until a carrying node meets the destination.

## III. SYSTEM MODEL-DTN

In DTN environment there is no centralized trusted authority, which consist multiple hops and encounters another node. The prevention of black hole attacks in DTN routing. This work consider friendship matrix, which represents social ties between the node. Here energy spend for maintaining the friends list and performing matching operations is very less because its computation energy is very lower than for DTN. When

node becomes selfish it only forwards the message when it's the friend of source or destination node. Malicious node can perform at trust related attacks such as self promoting attacks, bad mounting attacks, ballot stuffing. A malicious attacker can perform a random attacks for a evade detection here a random attack probability is introduced to reflect behaviour of random attack. When this value is equal to one when the attacker is reckless, when this value is less one it's the random attacker. A node's trust value assessed based on a direct trust evaluation and indirect trust information. Trust protocol independently executes each node and performs the direct trust assessment.

Define a trust node 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 model by which the trust value of node j evaluated by node i at time t, denoted as Ti,j(t), weighted average of healthiness, unselfishness, connectivity and energy.

$$T_{i,j}^{diect,x}(t) = \{ \text{I is a neighbor to j at i} \quad X \quad \text{, otherwise} \text{--------} \text{--- (1)}$$

Node communicate with multiple hops encounter another node they exchange to prevent blackhole attacks in DTN routing, Socially selfish nodes from malicious node act for its own interest including friends, groups, or communities, it will drop packets to save energy but may forward a packets with social ties with source and destination with friendship node. DTN routing functionally drops the packet in malicious node can perform trust related attacks. It can perform random attack to evade detection; the malicious attacker is reckless through bad-mounting attack and ballot stuffing which are mitigated in protocol design by trust recommendation threshold to fill the trust worthy recommenders. The trust of one node toward another node will execute the trust protocol independently, Direct trust assessment towards an encountered node based on detection mechanisms.

$$T_{i,j}^{X}(t) = \beta_1 T_{i,j}^{direct,x}(t) + \beta_2 T_{i,j}^{indi} \text{----- (3)}$$

## IV. TRUST EVALUVATION SCHEME:

In previous scheme novel trust management model is proposed which is divided into two parts: subjective trust evaluation model and trusted routing model. First, we setup a subjective trust evaluation model considering the behaviours of the dynamic nodes in the open environment and the influencing attributes of nodes' trustworthiness. Through the analytic hierarchy process (AHP) decision making on the trust influencing attributes and considering logic rules prediction, we can obtain a trust value for each node. The value not only provides a relative identification between the good nodes and the malicious or suspected nodes, but also offers a prediction of one's future behaviors. Then taking the trust value as the input, a trusted routing model is proposed.

$$T_{i,j}^{indirect,x}(t) = \{\sum m \in v(T_{i,m}^{X} X \quad / \quad e^{-\lambda d \Delta t} X T_{i,j}^{inc} \text{-------} \text{ (2)}$$

Based on the fuzzy dynamic programming theory, in a trusted routing model, we present a novel trusted routing algorithm which can kick out the untrustworthy nodes such that a reliable passage delivery route is obtained. As an application of the proposed trusted routing algorithm, a novel reactive routing protocol on the basis of the standard DSR protocol, called fuzzy trusted dynamic source routing (FTDSR) protocol is proposed. Finally, we compare the performances of the three routing protocols: DSR, TDSR and our FTDSR protocol, using the NS-2 simulator. The experimental results show that our routing model present higher detection ratio for malicious nodes. Moreover, FTDSR guarantees a higher packet delivery ratio and the network throughput effectively when compared to other protocols

$$T_{i,j}(t) = \quad + \quad (t) \quad + \quad W_2 T_{i,j}^{energy}(t) + W_4 T_{i,j}^{cool}(t) \text{ ---------- (3)}$$

$$T_{i,j}^{indirect,x}(t) = \{\sum m \in v(T_{i,m}^{X} X \quad / \quad e^{-\lambda d \Delta t} X T_{i,j}^{inc} \text{ ---------- (4)}$$

## V. IMPLEMENTATION:

To detect the sinkhole node in the route by applying timer or by not getting any acknowledgement from any other node in the route. Since the middle node is the sinkhole node it doesn't pass the data to the next node and source node never gets any data acknowledgement from the destination node. So it will suspect the intermediate node as the sinkhole node and it select the alternative, smallest path in the same region and transfer the data. The sinkhole and the remedy of the sinkhole are given in the following manner. The alternate method makes some packet may get loss due to the time, size of the date and length of the route. Source node and 6 is the destination node, when 0 starts transmitting the data to 6 through 3, 5 the node 3 is getting all the information and not transmitting to the other nodes. It is behaving like a sink and holding all the data by itself.

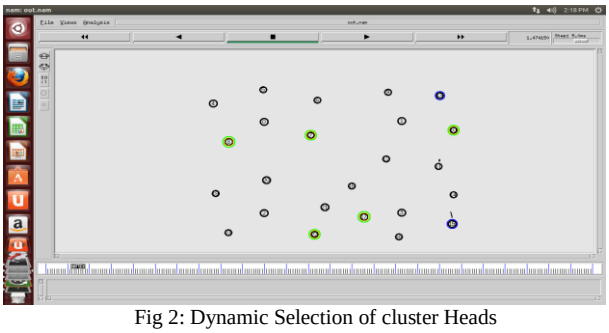

Fig 2: Dynamic Selection of cluster Heads

is waiting for destination node after sometime the node is suspecting node 3 in sinkhole attack

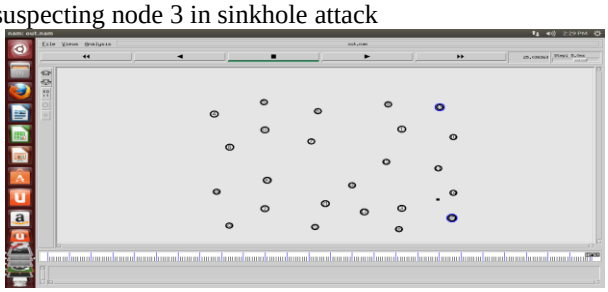

Fig 3: Packet Loss

In the above diagram it shown that intruder has occurred at the time of 70, the node 7 is having the highest energy level. And the leader is very near to the node where data is getting passed. Now the node7 is near to the source node 4 and it having the energy value high than other nodes and monitoring the other nodes ID and location.

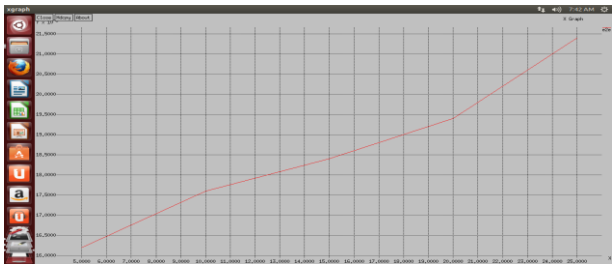

Fig 4: Number Nodes Vs Energy Values

The Number of Leader nodes and the attacker nodes are depending upon the IDS which we are deploying in the network. Since all the Leaders are acting as a monitoring nodes, the number of attacker getting reduced the performance is improved. The ratio of the attack node in a WSN is analyzed and given in the following table. Table 1 - 14% of attack nodes appears in a WSN.

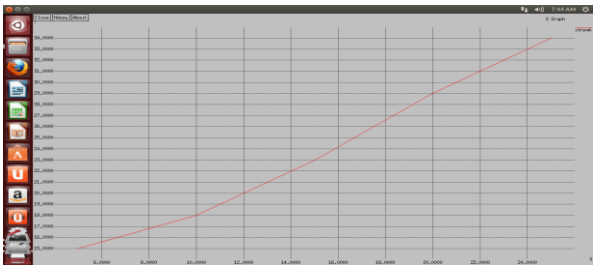

Fig 5: Simulation Time Vs Packet Delivery Ratio

The maximum delivery ratio obtainable when the system operates under the best trust formation setting identified. We see that the delivery ratio remains high even as the % of malicious nodes increases to as high as 45%. This to some extent demonstrates the resiliency property of our trust-based routing protocol against malicious attacks.

## VI. RESULT AND DISCUSSION

In the network, the wireless sensor network has the trust management designs by a novel model-based analysis methodology via extensive simulation. Specifically we develop a mathematical model based on continuous-time semi-Markov stochastic processes (for which the event time may follow any general distribution) to define a DTN consisting of a large number of mobile nodes exhibiting heterogeneous social and QoS behaviours. During the testing and debugging phase, a system would be tested with its anticipated operational profile to reveal design faults. Failures are detected and design faults causing System failures are removed to improve the system reliability. The operational profile of a DTN system specifies the operational and environmental conditions. Typically this would include knowledge regarding hostility such as the expected % of misbehaving nodes and if it is evolving the expected rate at which nodes become malicious or selfish or even the expected % of misbehaving nodes as a function of time.

During the forwarding of the message to the destination, the rate at which power is consumed by the cluster head will be calculated based on the energy model. The process will remove the route from the routing table of the source, which will lead the source node to initiate the new discovery process and find a new path to the destination node through the new cluster.

## VII. CONCLUSION:

A novel trust management model has been proposed. First, we use AHP theory and logic rules prediction method to establish a new trust evaluation model which is used to evaluate the trust of nodes. Then taking the trust value as the input, a trusted routing model is proposed. Based on the dynamic programming theory, in trusted routing model, we present a novel trusted routing algorithm which can kick out the untrustworthy nodes such that a reliable passage delivery route is obtained. As an application of the proposed trusted routing algorithm, a novel reactive routing protocol on the basis of the standard AODV protocol, called T-AODV protocol is proposed which is used to discover trustworthy forward paths and alleviate the attacks from malicious nodes. The successful test on the comparison of AODV and DSR shows that our performance evaluation mechanism developed by this project is really effective for scalable performance test in NS-2. It also could be easy to use for measure the network routing protocols' performance, meanwhile, since it has the fix model of analysis the trace file, with some minor modification, it will then be apply to measure other kinds of stuffs with the whole network simulation. However, since we now only explore some important fields of the trace file, in the future, need to provide the measurement with other fields of the trace file and analysis more details on the things what we can get in the trace file.

**REFERENCES**


[1] Ing-Ray Chen, Fenye Bao, Moon Jeong Chang, and Jin-Hee Cho, "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing*," IEEE Transactions on Parallel an Distributed Systems, 2013.*

[2] E. Ayday, H. Lee, and F. Fekri, "An Iterative Algorithm for Trust Management and Adversary Detection for Delay Tolerant Neworks," *IEEE Transactions on Mobile Computing, vol. 11, no. 9,*Sept. 2012, pp. 1514-1531.

[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 Transactions on Parallel and Distributed Systems, 2013.*

[4] 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.*

[5] E. M. Daly, and M. Haahr, "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs," *IEEE Transactions on Mobile Computing, vol. 8, no. 5, May 2009, pp.* 606-621.

[6] K. Paul and D. Westhoff, "Context aware detection of selfish nodes in dsr based ad-hoc networks," Proceedings of IEEE Global Telecommunications Conference (GLOBECOM02), pp. 178–182, 2002.

[7] 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.

[8] H. Al-Hamadi, and I. R. Chen, "Dynamic Multisource Multipath Routing for Intrusion Tolerance and Lifetime Maximization of Autonomous Wireless Sensor Networks," IEEE 11th Symposium on Decentralized Autonomous Systems, Mexico City, March 2013.

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

[10] I. R. Chen, F. Bao, M. Chang, and J. H. Cho, "Trust Management for Encounter-Based Routing in Delay Tolerant Networks," *IEEE Global Communications Conference*, Miami, Florida, USA, Dec. 2010, pp. 1-6

[11] 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.