International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 10 91 – 94

Trust Management for Secure Routing Forwarding Data Using Delay Tolerant Networks

K. Aravindha[1]
(Research Scholar)
Dept of Computer Science
Tamil University,Thanjavur,
Thanjavur,Tamil Nadu,India.
e-mail:aarrmsc@gmail.com

A. Senthil Kumar[2]
(Asst.Professor)
Dept of Computer science,
Tamil University, Thanjavur,
Thanjavur, Tamil Nadu,India.
e-mail:erodesenthilkumar@gmail.com

Abstract: Delay Tolerant Networks (DTNs) have established the connection to source and destination. For example this often faces disconnection and unreliable wireless connections. A delay tolerant network (DTNs) provides a network imposes disruption or delay. The delay tolerant networks operate in limited resources such as memory size, central processing unit. Trust management protocol uses a dynamic threshold updating which overcomes the problems .The dynamic threshold update reduces the false detection probability of the malicious nodes. The system proposes a secure routing management schemes to adopt information security principles successfully. It analyzes the basic security principles and operations for trust authentication which is applicable in delay tolerant networks (DTNs).For security the proposed system identifies the store and forward approach in network communications and analyzes the routing in cases like selfish contact and collaboration contact methods. The proposed method identifies ZRP protocol scheme and it enhances the scheme using methods namely distributed operation, mobility, delay analysis, security association and trust modules. This security scheme analyzes the performance analysis and proposed algorithm based on parameter time, authentication, security, and secure routing. From this analysis, this research work identifies the issues in DTNs secure routing and enhances ZRP (Zone Routing Protocol) by suggesting an authentication principle as a noted security principle for extremely information security concepts.

Keywords: *Delay Tolerant Networks (DTNs), selfish attack, Network security, Data security, Trust Management.*

*****

I. INTRODUCTION OVERVIEW:

Wireless Delay Tolerant Network (DTNs) is a new Networks class which is characterized by a long message delay and lack of a fully connected path between the source and the target nodes. As a result, the use of mobile node acting as a buffer
between the one to other end and behave as a store and forward approach. The message sending is an opportunistic procedure because the messages are sent in an opportunistic way. Because of its characteristics wide range of useful applications have been developed for DTNs and enable a new class of networking applications in the wireless network interface which increases popularity of mobile devices. DTNs can be used for developing low-cost internet services on remote area moreover it can be used for DTNs for local advertising, location-based information collection such as traffic reports and parking information. However, practical DTNs implementation is questionable because its characteristics making them vulnerable to serious security threats.

In the system every node predicted that intermediate nodes are relaying the message properly. However malicious node not carries the message properly in the network which causes multi-hop communications to fail and detection of their presence may be hard. DTNs relay carries sharing which is the essential requirement, but this cannot be guarantee because selfish nodes can avoid participating for other messages. On other hand malicious node creates the black hole which carries out attacks by deliberately dropping messages. Overcome these attacks is a real challenge due to the connectivity and distributed nature of DTNs. DTNs are resource constrained in nature to save its own resource and nodes may develop selfish behavior. In which its drop the packet of other nodes to maximize its own credit or benefits. Such nodes increase the message drop probability and reduce the message delivery rate. In propose a dynamic trust based approach protect network from black hole a selfish attacks. The rest of the paper is organized as follows: the second section provides a brief discussion of the most recent relative literature of DTNs and the system model is defined third section. The fourth section explains the proposed algorithm and the simulator results and fifth section explain about conclusion and future work on the basis of the simulation results presented in fourth section.

A major challenge of a provenance-based system is that it must define against attackers who may modify or drop messages including provenance information or

disseminate fake information. Leveraging the interdependency of trust in information source and information itself based on the concept of provenance, this work proposes a provenance based trust framework, called Trust model that aims to answer the challenge. The design goals of PROVEST are (1) minimizing trust bias ;(2)minimizing communication cost caused by trust assessment; and(3)maximizing quality-of-services (Qos) by minimizing message delivery delay and maximizing correct message delivery ratio.

The security overhead incurred by forwarding history checking is critical for a DTN since expensive security operations will be translated into more energy consumption, which represents a fundamental challenge in resource- constrained DTN. The proposed trust scheme is inspired from the Inspection Game, a game theory model in which an inspector verifies if another party, called inspective, adheres to certain legal rules. In this model, the inspective has a potential interest in violating the rules while the inspector may have to perform the partial verification due to the limited verification resources. Therefore, the inspector could take advantage of partial verification and corresponding punishment to discourage the misbehaviors of inspectors. Furthermore, the inspector could check the inspective with a higher probability than the Nash Equilibrium points to prevent the offences, as the inspective must choose to comply the rules due to its rationality. Inspired by Inspection Game ,to achieve the tradeoff between the security and detection cost,iTrust introduces a periodically available Trust Authority(TA), which could launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. Then TA could punish or compensate the node based on its behaviors.

A. Objective:

The main objective is to develop a robust trust mechanism and an efficient and low cost malicious node detection technique for DTNs. Avoid state explosion problems and to improve solution efficiency for realizing and describing the behaviors of each node and obtaining objective trust values. It provides a critical analysis of the main unresolved research challenges. The message moves to a new node when it appears in the range, similarly the messages reach their destinations.

II. SYSTEM ANALYSIS

A. Existing System:

The previous strategy cannot work in an environment in which the nodes save a high probability of being selfish to other nodes. Finally a comparative analysis of our proposed routing with previous routing protocols is also performed. 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. The average delay occurred to deliver a message and the ratio of correct message delivery. The previous trust model in by considering the following enhancements trust is scaled in [0; 1] as a real number, trust evidence, either direct or indirect evidence, is modeled by the beta distribution with evidence filtering.

Disadvantage*:*

- Node not carries the message properly in the network.
- TA probability cannot be guaranteed if network size is large.
- Encounter based evidence exchange among nodes may not be always possible.

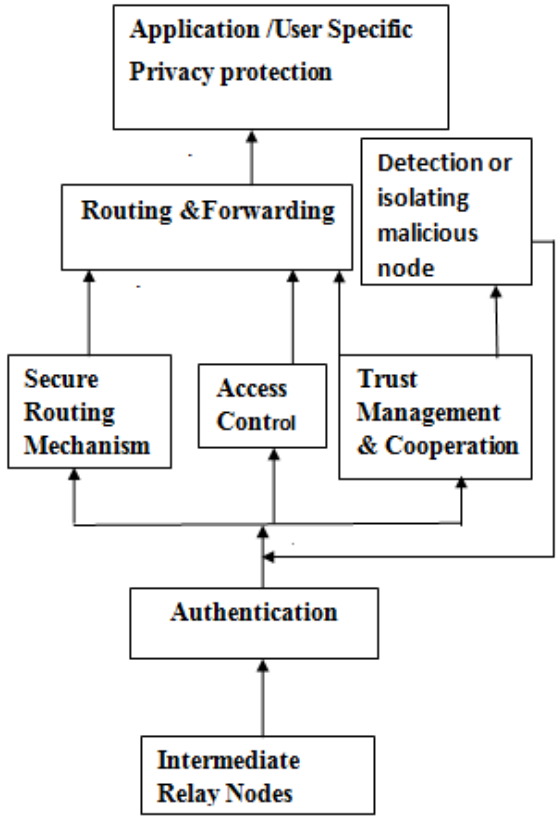
B.Proposed System:

DTNs can be used for developing low-cost internet services on remote area moreover it can be used for vehicle DTNs for local advertising. Location-based information collection such as traffic reports and parking information. Reputation is also used in Social Selfishness Aware Routing (SSAR) the performance of the node is not affected by the not well-behaved nodes. First check the willingness of receiving node if it is ready then the message with higher delivery probability in the network is transferred. To measure low actively node forwards others messages the node's trust value.

Advantage:

- The nodes with high trust values are preferable in data forwarding to avoid the attackers that are not participating in routing process.
- It increases the probability of packet transfer through malicious node by proving good recommendations to the bad nodes.
- To receive the information encrypted the public identifier is used based on identity –based encryption

III. SYSTEM ARCHITECTURE



.

IV. MODULE SPECIFICATIONS: 1. A. Distributed operation

For the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in an Ad hoc Network should collaborate amongst themselves and each node acts as relay as needed, to implement functions e.g. security and routing. Mobile Ad hoc Networks (DTNs) are infrastructure less networks without fixed routers, which are designed by a cluster of wireless nodes. Each of the nodes in a DTN can assume the responsibility of forwarding packets. Nodes in DTNs can move from one location to other and can be connected dynamically.

B. Mobility

A wireless MANET is a collection of communication nodes that wants to communicate with each other, but has no fixed infrastructure and no re-determined topology of links. Mobile ad hoc network is a collection of wireless mobile nodes dynamically forming a network topology without the use of any existing network infrastructure. The purpose of present work is to compare the performance of AODV,DSR and DSDV MANET protocols for different number of nodes and mobility with different traffic channels CBR and FTP.The AODV and DSR are reactive or On demand routing protocol and DSDV is a proactive or table driven routing protocol. The performance metrics considered in this work includes packet delivery ratio, throughput and average end-to-end delay.

C. Delay Analysis

In this module consider two mobile nodes, each move at constant speed v in a randomly and independently chosen direction. Therefore, without loss of generality, may assume that one is fixed and the other node moves with an average relative velocity. Each segment si is a delay induced by the action taken by the i-th node on the path. Notice that since node motions are any node in the journey can be interchanged with any other node. Therefore, the probability distribution of a journey only depends on the size k and not on the location of nodes on the map.

D. Security Association

Routing protocols can be classified as: Table-driven (proactive), proactive protocols also referred as “table driven” routing protocols. Here, each node keeps comprehensive information about the network topology by constantly estimating routes to all the nodes.

E. Trust

This approaches for solving the performance issues such as changes in topology, Energy consumption of mobile nodes, delay, routing overhead, message delivery time, Throughput, packet delivery ratio, security of networks and mobility management. To provide a perception of solutions for these issues, this study concentrates on various methodologies such as effective hierarchical routing algorithm, Link stability with energy aware Multipath routing protocol, path encounter rate metric and Trust-based source routing protocol. Effective hierarchical routing algorithm computes the route and has decreased the load of routing protocols.

V. CONCLUSION:

In this paper, we first classified the selfish behavior in DTNs and then existing strategies for preventing selfish behavior. we subsequently analyzed the mechanisms and explored techniques of the strategies. Further, we find out the problems in previous technique. the previous strategy cannot work in an environment in which the node saves a high probability of being selfish to other nodes.But,we conducted an experiment to investigate the performance of the representative strategies in each category. The results of our experiment illustrate that the performance of proposed strategies outperforms the previous technique.

REFERENCES

[1] Mohamed Elsalih Mahmoud, MrinmoyBarua, and Xuemin (Sherman) Shen,"SATS: Secure Data Forwarding Scheme for Delay-Tolerant wireless Networks", IEEEGlobecom-Communication and system security, 2011.

[2] Ing-Rray Chen, Fenyebao,Moonjeong Chang,and Jin-Hee Cho, "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing",IEEE TRANSACTION,2013

[3] Ing-Ray Chen, Fenyebao, Moonjeong Chang, Jin-Hee Cho, "Trust Management for Encounter-Based Routing in Delay Tolerant Networks", Standard from 298(rev.8-98) prescribed by ANSI-std z39-18, 2010

[4] E.Bulut, B. Szymanski "Secure Multi-Copy Routing In Compromised Delay Tolerant Networks", Wireless Personal Communication, vol.73(1), November 2013, pp.149-168.

[5] WANG Cheng–jut, GONG Zheng-hu,TAO Yong, ZHANG Zi-wen,ZHAO Bao-kang "CRSG: a congestion control routing algorithm for security defense based on social psychology and game theory in DTN", J.cent.south Univ.(2013)20:44-450

[6] Ying Zhu, Bin Xu, Xinghua Shi and Yu Wang "a Survey of Social-Based Routing in Delay Tolerant Networks: Positive and Negative Social Effects", IEEE COMMUNICATIONS SURVEY&TUTORIAL, VOL.15, NO.1, FIRST QUARTER 2013.

[7] Bin Bin Chen & MunChoon Chan,"Mobicent: a Credit Based Incentive System for Disruption Tolerant Network", National University of Singapore,2008

[8] Forrest Warthman, Delay Tolerant Networks (DTNs), A Tutorial, March 2008

[9] Haojin Zhu,XiaodongLin,Rongxing Lu,Yanfei Fan,and Xuemin(Sherman) Shen,"SMART:A Secure Multilayer Credit-Based Inactive Scheme for Delay-Tolerant Networks",IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY,VOL.58,OCTOBER 2009

[10] Haojin Zhu, Member, Suguo Du, Zhaoyugao, Mianxiong Dong, IEEE, and Zhenfu Cao "A Probabilistic Misbehavior Detection Scheme towards Efficient Trust Establishment in Delay-Tolerant Networks", IEEE, 2013

[11] Ting Ning, Zhipeng Yang, Hongyi Wu, and Zhu Han ,"Self-Interest-Driven Incentives for Ad Dissemination in Autonomous Mobile Social Networks", 2013 Proceedings IEEE INFOCON

[12] LIFEI WEI, HAOJIN ZHU,ZHENFU CAO,XUEMIN SHEN,"SUCCESS:A Secure User-centric and social aware Reputation based Incentive scheme for DTNs",15 October 2011,Grant No.61033014,National Natural Science Foundation of china.