ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

Efficient Trust Establishment in Delay-Tolerant Networks Based on iTrust Protocol

S.P.Vijayaragavan[1], E.Vadivel[3], M.Sriram[2]

[1] Assistant Professor, Department of EEE, Bharath University, Chennai, India

[2]Assistant Professor, Department of CSE, Bharath University, Chennai, India

[3]PG Student, Department of CSE, Bharath University, Chennai, India

ABSTRACT: We propose iTrust introduces a periodically available 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. We assume that each node must pay a deposit amount before it joins the network, and the deposit will be paid back after the node leaves if there is no misbehavior activity of the node. TA could ensure the security of DTN routing at a reduced cost. If any Node leaves or Joins the Network, then the Key will be alerted and send as E mail Alert to the Corresponding Nodes of the Network. Previous Nodes cannot access the data from the newly joined Network. We assume that each node must pay a deposit amount before it joins the network, and the deposit will be paid back after the node leaves if there is no misbehavior activity of the node. TA could ensure the security of DTN routing at a reduced cost.

KEYWORDS: DTNs, TA, Routing, Dynamic Detection.

I. INTRODUCTION

This Delay tolerant networks (DTNs), such as sensor networks with scheduled intermittent connectivity, vehicular DTNs that disseminate location-dependent information (e.g., local ads, traffic reports, parking information), and pocket-switched networks that allow humans to communicate without network infrastructure, are highly partitioned networks that may suffer from frequent disconnectivity.[1-3] In DTNs, the in-transit messages, also named bundles, can be sent over an existing link and buffered at the next hop until the next link in the path appears (e.g., a new node moves into the range or an existing one wakes up).[4] This message propagation process is usually referred to as the "store-carry-and-forward" strategy, and the routing is decided in an "opportunistic" fashion. In DTNs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data (e.g., sufficient buffers and meeting opportunities). Routing misbehavi can be caused by selfish (or rational) nodes that try to maximize their own benefits by enjoying the services provided by DTN while refusing to forward the bundles for others, or malicious nodes that drop packets or modifying the packets to launch attacks.[5-6]

The recent researches show that routing misbehavi will significantly reduce the packet delivery rate and, thus, pose a serious threat against the network performance of DTN. [7]Therefore, a misbehavi detection and mitigation protocol is highly desirable to assure the secure DTN routing as thell as the establishment of the trust among DTN nodes in DTNs. In this project, the propose iTrust, a probabilistic misbehavi detection scheme to achieve efficient trust establishment in DTNs. Different from existing works that only consider either of misbehaviour detection or incentive scheme, the jointly consider the misbehavi detection and incentive scheme in the same framework. The proposed iTrust scheme is inspired from the inspection game, a game theory model in which an inspector verifies if another party, called inspected, adheres to certain legal rules. In this model, the inspectee has a potential interest in violating the rules while the inspector may have to perform the partial verification due to the limited verification res ces. Therefore, the inspector could take advantage of partial verification and corresponding punishment to disc age the misbehavi of inspected. [8]Furthermore, the inspector could check the inspected with a higher probability than the Nash Equilibrium points to prevent the offences, as the inspected must choose to complete the rules due to its rationality.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

II. PROBLEM IDENTIFICATION

DTNs to deal with find out the malicious, selfish misbehaving nodes and genuine loss nodes.[9-11] Selfishness is social selfishness, as very often humans carrying communication devices in a DTN are socially selfish to outsiders but unselfish to friends. Maliciousness refers to malicious nodes performing trust-related attacks to disrupt DTN operations built on trust. The aim to identify the malicious node and selfish node based on checking node energy level and buffer level using multi hop forwarding algorithm. But it is time consuming process.

a. Existing System

In the existing system, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data. Routing misbehavior can be caused by malicious nodes that drop packets or modifying the packets to launch attacks. Thus, pose a serious threat against the network performance of DTN.[12-14]

2.2 Proposed System

In the proposed system**,** the propose iTrust introduces a periodically available 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. It assume that every node must pay a fund before joining the network, and the deposit will be paid back after the node leaves if there is no misbehavior activity of the node. TA could ensure the security of DTN routing at a reduced cost.

III. ARCHITECTURE DIAGRAM

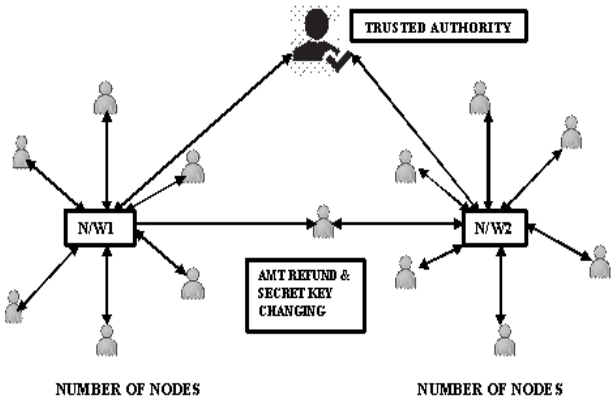

Fig 1. Data Transfer Diagam

NETWORK CONSTRUCTION

This module is developed in order to create a dynamic network. In a network, nodes are interconnected with the Trusted Authority, which is monitoring all the other nodes. All nodes are sharing their information with each others.

USER DEPOSITE

Each node is assumed to have a unique ID and a corresponding public/private key pair. The assume that each node must pay a deposit before it joins the network, and the deposit will be paid back after the node leaves if there is no misbehavior activity of the node.

MISBEHAVIOR DETECTION IN DTNs

TA contain the contact history of every node that could prevent the black hole or gray hole attack because the nodes with sufficient contact with other users fail to forward the data will be regarded as a malicious or selfish

TA(TRUSTED AUTHORITY)

TA is a trusted authority is used monitor all the node in different group and it also contain the up streaming and down streaming history of every node so that it route the packet to the correct destination.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

EMAILALERT

If any node quit form the network or else any new node join in the network the group id is changed and it send to every group through the email. So that the node quit or join can use the old group id.

IV. FLOW CHART

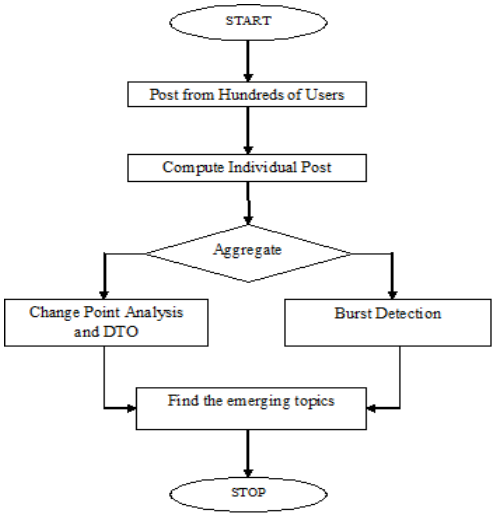

Fig 2. Flow Chart

V. DATA FLOW

Level 0

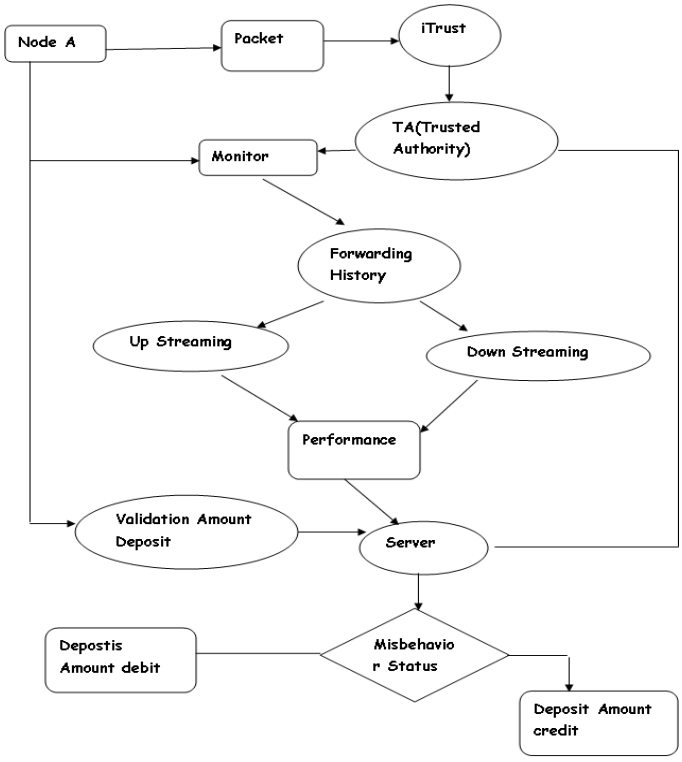

Fig 3.a Route Transfer

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

Level 1

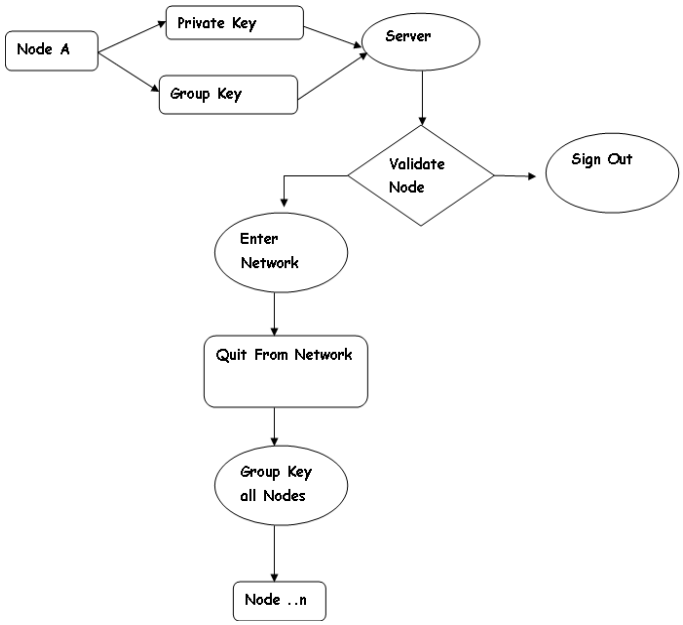

Fig 3.b Route Transfer

USE CASE DIAGRAM

A use case diagram is a type of behavi al diagram created from a Use-case analysis. The purpose of use case is to present overview of the functionality provided by the system in terms of actors, their goals and any dependencies between those use cases.

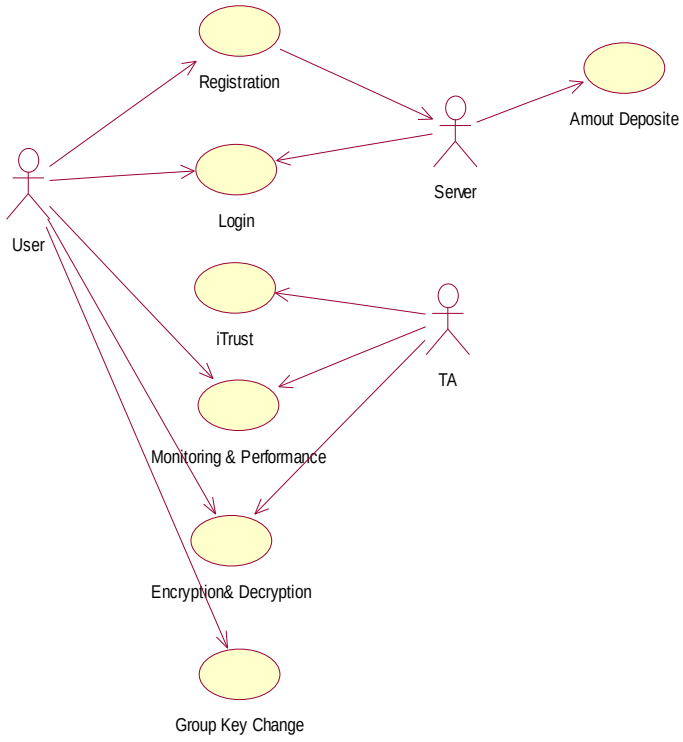

Fig 4. Use case diagrams of WS

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

VI. ALGORITHM SPECIFICATION

Key-scheduling algorithm (KSA)

The key-scheduling algorithm is used to initialize the permutation in the array "S". "keylength" is defined as the number of bytes in the key and can be in the range $1 \leq$ keylength ≤ 256, typically between 5 and 16, corresponding to a key length of 40 – 128 bits. First, the array "S" is initialized to the identity permutation. S is then processed for 256 iterations in a similar way to the main PRGA, but also mixes in bytes of the key at the same time.

Pseudo-random generation algorithm (PRGA)

For as many iterations as are needed, the PRGA modifies the state and outputs a byte of the keystream. In each iteration, the PRGA increments i, looks up the ith element of S, S[i], and adds that to j, exchanges the values of S[i] and S[j], and then uses the sum S[i] + S[j] (modulo 256) as an index to fetch a third element of S, (the keystream value K below) which is XORed with the next byte of the message to produce the next byte of either cipher text or plaintext. Each element of S is swapped with another element at least once every 256 iterations.

RC4-based random number generators

Several operating systems include arc4random, an API originating in OpenBSD providing access to a random number generator originally based on RC4. In Open BSD 5.5, released in May 2014, arc4random was modified to use ChaCha20. Hothever, as of September 2014, implementations of arc4random in FreeBSD, NetBSD, Linux's libbsd, and Mac OS X are still based on RC4.

Proposed new random number generators are often compared to the RC4 random number generator.

Unfortunately, several attacks on RC4 are able to distinguish its output from a random sequence.

Implementation

Many stream ciphers are based on linear feedback shift registers (LFSRs), which, while efficient in hardware, are less so in software. The design of RC4 avoids the use of LFSRs, and is ideal for software implementation, as it requires only byte manipulations. It uses 256 bytes of memory for the state array, S[0] through S[255], k bytes of memory for the key, key[0] through key[k-1], and integer variables, i, j, and K. Performing a modular reduction of some value modulo 256 can be done with a bitwise AND with 255 (which is equivalent to taking the low-order byte of the value in question).

Test vectors

These test vectors are not official, but convenient for anyone testing their own RC4 program. The keys and plaintext are ASCII, the key stream and cipher text is in hexadecimal.

Unlike a modern stream cipher (such as those in eSTREAM), RC4 does not take a separate nonce alongside the key. This means that if a single long-term key is to be used to securely encrypt multiple streams, the cryptosystem must specify how to combine the nonce and the long-term key to generate the stream key for RC4. One approach to addressing this is to generate a "fresh" RC4 key by hashing a long-term key with a nonce. Hothever, many applications that use RC4 simply concatenate key and nonce; RC4's theak key schedule then gives rise to related key attacks, like the Fluhrer, Mantin and Shamir attack (which is famous for breaking the THEP standard).

Because RC4 is a stream cipher, it is more malleable than common block ciphers. If not used together with a strong message authentication code (MAC), then encryption is vulnerable to a bit-flipping attack. The cipher is also vulnerable to a stream cipher attack if not implemented correctly. Furthermore, inadvertent double encryption of a message with the same key may accidentally output plaintext rather than cipher text because the involuntary nature of the XOR function would result in the second operation reversing the first.

It is noteworthy, hothever, that RC4, being a stream cipher, was for a period of time the only common cipher that was immune to the 2011 BEAST attack on TLS 1.0. The attack exploits a known theakness in the way cipher block chaining mode is used with all of the other ciphers supported by TLS 1.0, which are all block ciphers.

VII. CONCLUSIONS

In this project, we propose a probabilistic misbehaviour detection scheme (iTrust), which could reduce the detection overhead effectively. The model it as the inspection game and show that an appropriate probability setting could assure the security of the DTNs at a reduced detection overhead. simulation results confirm that iTrust will reduce transmission overhead incurred by misbehaviour detection and detect the malicious nodes effectively. future work will focus on the extension of iTrust to other kinds of networks.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

REFERENCES

[1] Haojin Zhu, Suguo Du, Zhaoyu Gao, Mianxiong Dong, and Zhenfu Cao, Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 1, JANUARY 2014
[2] Mahalakshmi K., Prabhakar J., Sukumaran V.G., "Antibacterial activity of Triphala, GTP & Curcumin on Enterococci faecalis", Biomedicine, ISSN : 0970 2067, 26(Mar-4) (2012) pp. 43-46.
[3] Bhuvaneswari B., Hari R., Vasuki R., Suguna, "Antioxidant and antihepatotoxic activities of ethanolic extract of Solanum torvum", Asian Journal of Pharmaceutical and Clinical Research, ISSN : 0974-2441, 5(S3) (2012) pp. 147-150.
[4] hariharan V.S., Nandlal B., Srilatha K.T., "Efficacy of various root canal irrigants on removal of smear layer in the primary root canals after hand instrumentation: A scanning electron microscopy study", Journal of Indian Society of Pedodontics and Preventive Dentistry, ISSN : 0970-4388, 28(4) (2010) pp.271-277.
[5] Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012.
[6] T. Hossmann, T. Spyropoulos, and F. Legendre, "Know the Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing," Proc. IEEE INFOCOM '10, 2010.
[7] R. Lu, X. Lin, H. Zhu, and X. Shen, "Pi: A Practical Incentive Protocol for Delay Tolerant Networks," IEEE Trans. Wireless Comm., vol. 9, no. 4, pp. 1483-1493, Apr. 2010.
[8] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay- Tolerant Networks," Proc. IEEE INFOCOM '10, 2010.
[9] Sathyanarayana H.P., Premkumar S., Manjula W.S., "Assessment of maximum voluntary bite force in adults with normal occlusion and different types of malocclusions", Journal of Contemporary Dental Practice, ISSN : 1526-3711, 13(4) (2012) pp.534-538.
[10]]Selva Kumar S., Ram Krishna Rao M., Deepak Kumar R., Panwar S., Prasad C.S., "Biocontrol by plant growth promoting rhizobacteria against black scurf and stem canker disease of potato caused by Rhizoctonia solani", Archives of Phytopathology and Plant Protection, ISSN : 0323-5408, 46(4) (2013) pp.487-502.
[11] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 8, pp. 828-836, 2009.
[12] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET Based Smart Parking Scheme for Large Parking Lots," Proc. IEEE INFOCOM '09, Apr. 2009.
[13] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks," IEEE Trans. Wireless Comm., vol. 17, no. 10, pp. 3858- 3868, Oct. 2008.
[14] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom '00, 2000.
[15] Thooyamani, K.P., Khanaa, V., Udayakumar, R., "Wireless cellular communication using 100 nanometers spintronics device based VLSI", Middle - East Journal of Scientific Research, v-20, i-12, pp:2037-2041, 2014.
[16] Vanangamudi, S., Prabhakar, S., Thamotharan, C., Anbazhagan, R., "Dual fuel hybrid bike", Middle - East Journal of Scientific Research, v-20, i-12, pp:1819-1822, 2014.
[17] Udayakumar, R., Kaliyamurthie, K.P., Khanaa, Thooyamani, K.P., "Data mining a boon: Predictive system for university topper women in academia", World Applied Sciences Journal, v-29, i-14, pp:86-90, 2014.
[18] Satheesh, S., Lingeswaran, K., "High efficiencytransformer less inverter for single-phase photovoltaic systems using switching converter", Middle - East Journal of Scientific Research, v-20, i-8, pp:956-965, 2014.
[19] Vijayaragavan, S.P., Karthik, B., Kiran Kumar, T.V.U., "A DFIG based wind generation system with unbalanced stator and grid condition", Middle - East Journal of Scientific Research, v-20, i-8, pp:913-917, 2014.