Volume : 4 | Issue : 3 | March 2015 • ISSN No 2277 - 8179

Efficient Trust Establishment Using a Probabilistic Delinquency Detection Scheme in Delay Tolerant Networks.

Engineering

KEYWORDS : Malicious attack, Selfish attack, Black hole attack, Game theory, Safe route discovery.

S.Padmapriya	Anna University, S.A Engineering College, Department of Computer Science and Engineering
R.Saranya	Anna University, S.A Engineering College, Department of Computer Science and Engineering

ABSTRACT

Delay tolerant network communicates without network infrastructure that suffers from frequent disconnectivity. Malicious attack, Selfish attack and Black hole attack represent serious threats against routing in DTNs. A Provocation to the DTN is to design a delinquency detection scheme. iTrust is a delinquency detection scheme designed for unassailable DTN routing towards trust establishment. Trusted authority is introduced to percept nodes behavior based on the collected routing affirmation and anticipated study. iTrust is divided into two different phases:- 1) Routing affirmation generating phase. 2) Routing affirmation inspecting phase. Nodes generate contact and data forwarding affirmation in the generation phase. The trusted authority differentiates the normal nodes from the delinquency nodes in the inspecting phase. The results from simulation confirm that iTrust reduces transmission overhead incurred by delinquency detection and detects effectively.

INTRODUCTION

Delay tolerant networks are designed to provide reliable transmission, interoperable communications between wide ranges of networks. The main drawback of DTN is "intermittent connectivity" and security. DTNs are conceived originally to support the Inter Planetary Internet (IPN). The growing demand for new network architecture was to support communications in the context of long propagation delay, low data rates, and intermittent connectivity. The IPN found a solution, suggesting new network architecture to support reliable transmission between any stations on earth and the satellites with an overlay network. The path and link consists of certain characteristics such as high error, asymmetric rate, disconnection, long and variable delay. Interoperability on a large scale network is rarely designed in challenged network. It is because these networks seem to be more simple and local in scope. Partitions occur due to geographic distance and less signal strength. The security approach is only to secure the end points of the network which is not sufficient due to link capacity limit. So, the access to the service is protected at the earliest point in the topology. The end system possesses limited longevity where the end node frequents high integration, low power consumption, low-cost device, lack of long usage due to environmental dangers and power exhaustion. The transmission schedule of low duty cycle operation receives a special consideration in the routing decision as the duty cycles of the node may be low, to achieve reasonable longevity of the entire network. There is frequently limitation in memory and processing capability of the node. If the network is designed for reliability then the end node should empty the retransmission rather than waiting for an end-to-end acknowledgement.

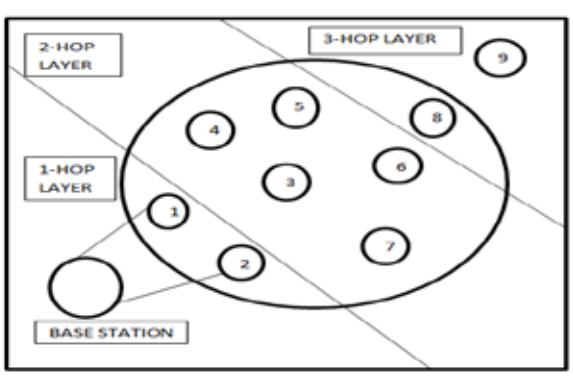

Figure.1: Distributed Collection of Networked Sensors in DTN

The above diagram explains about the hopping factor practiced by DTN. Nodes 1 and 2 present in the first hop layer can be reached in a single hop from the base station and so the region is "1-Hop layer". Nodes 3 to 7 can be reached only after touching nodes 1 and 2, so it is reached in 2 hops and the region is known as "2-Hop layer". Nodes 8 and 9 are present a little away and can only be reached after touching the first and second hop layers. So, the region surrounding the nodes 8 and 9 is known as the "3-Hop layer".

Nodes misbehavior is detected, where it drops packets intentionally even if the capability to forward data is present. Misbehavior is being caused by 3 different types of attacks.

- Selfish Attack
- Malicious Attack
- Black Hole Attack

CASE STUDY

SYSTEM ARCHITECTURE

A Normal DTN is considered where all the individual users own a mobile device. Each node is identified by a unique ID or number with either a public or private key. Assuming each node to pay before joining the DTN, it will be paid back if there exists no misbehavior by that particular node. Introducing the Trusted Authority (TA), it periodically checks for the behavior of all the nodes in the DTN. For a particular misbehavior detection, the TA requests for the forwarding data to the entire network. Hence, all the nodes submit the forwarding history evidences to the TA.

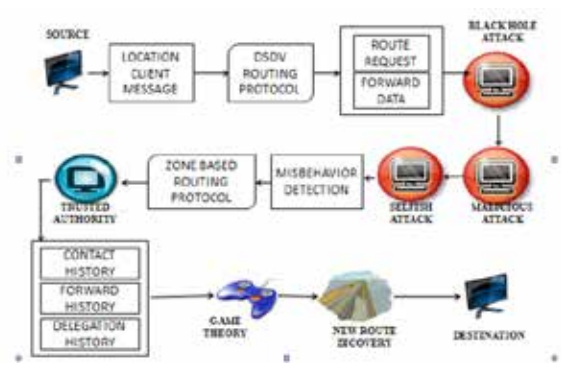

Figure.2: System Architecture

4.1 Game Theory: Game theory is the study of the ways in which strategic interactions among rational players produce outcomes with respect to the preferences or utilities of those players, none of which might have been intended by any of them. Game theory was created and organized by john van Neumann and Oscar Morgenstern in the year 1944. Game theory attempts to cite at the relationship between the wards in a particular model and depicts their optimal decisions. A frequently cited game theory example is with the prisoners. There are two brokers accused of fraudulence: Dev and maya. Both dev and maya are being inquired separately. Both of them want to minimize the time spent in jail. The dilemma varies as follows:

1) If dev pleads non convicted and maya confesses, maya will receive the short sentence of one year, and dev will have to stay in jail for the long sentence of five years.

2) If none makes any connotation they will both receive a punishment of two years.

3) If both of them decide to plead convicted and implicate their partner, they both will receive a punishment of three years.

4) If maya pleads non convicted and dev confesses, then Dev will receive a minimum punishment of one year, and maya will have to stay in jail for the punishment of maximum five years.

Obviously, conviction is the most attractive should the other plead non-convicted, since the punishment is only one year. However, if the other party also chooses to plead convicted, both will have to be punished for three years. On the other hand if both parties plead non-convicted they would have to be punished for two years in jail. Then, the risk of pleading non-convicted is a five-year punishment, where the other chooses to confess.

Node Detection and classification: M_n is the number of data sets for which the suspicious node is found and θ_{max} is a bound on the anticipation of the false positive detection of well behaving nodes, as if they are misbehaving. Willing to accept, i.e., by considering that a node that is detected with an anticipation that $\leq\theta_{max}$ is a perfect node. The value of α=0.0001 is set by default and be the classified error that is targeted. Classification of the monitored node as delinquency if

$$M_n > K(n) \tag{1}$$

where

$$K(n) = \begin{cases} \min\left\{k : \sum_{i=k+1}^{n} B_{n,\theta_{max}}(k) \leq \alpha\right\} & n\theta_{max} \leq 5 \\ n\theta_{max}\left(1 + \frac{\xi(\alpha)}{\sqrt{n}}\sqrt{\frac{1-\theta_{max}}{\theta_{max}}}\right) & \text{otherwise} \end{cases} \tag{2}$$

$B_{n,\theta_{max}}$ is binomial distribution with parameters and θ_{max} and $\xi(\alpha)$ is the $(1-\alpha)$ Quartile of normal distribution $\xi(0.0001) = 3.72$). As long as (1) is not true, the node is classified as well behaving. For the default parameter values, $n\theta_{max}\leq 5$ corresponds to $n\leq 83$.

Algorithm 1. The Proposed Delinquency Detection algorithm.

1: Start with n number of nodes
2: for the nodes m 1 to n do
3: generation of a random number mm from 0 to 10n _ 1
4: if mm=10n < pc then
5: question all the nodes including node m to provide affirmation about node m
6: if the Detection (m; TTtask; TTforward; ½t1; t2&; S; E) then
7: then give a punishment D to node m
8: else
9: supply node m the compensation x
10: end if
11: else
12: supply node m the compensation x
13: end if
14: end for

Modeling of the above described algorithm as an inspection game demonstrates that, by setting an appropriate detection delinquency threshold, achieves a lower detection overhead and still stimulates the nodes to forward the packets to all other nodes.

PROBLEMS IN EXISTING SYSTEM

Node misbehaves by dropping packets intentionally. Misbehaving nodes maximizes its own benefits. The security operations are more expensive and so get translated into more energy consumption. Transmission overhead cost and verification cost is very high.

Low duty cycle operation: The transmission schedule receives a special consideration in the routing decision as the duty cycle of the node may be less. This is to achieve reasonable longevity through the entire network. The pattern of the communication should be scheduled in advance due to power limitation.

Limited Resources: Limitation in memory and processing capability in the node is frequent. The end-node in the network should empty and buffer the retransmission quickly, other than waiting for an end-to-end acknowledgement.

Long and variable Delay: The queuing time of this network is extremely large, difficult to estimate. Source initiated transmission is expensive and it is also limited. Hence, the data is stored in a buffer or queue for a long potential period in each router even if there exist no direct path to the destination node.

Interoperability Consideration: Challenged networks gets rarely designed using interoperable large scale networks as it tends to be more simple and local in scope. Disconnection occurs due to geographic distance and lack of radio signal strength.

Security: The approach is only to secure the end points of the network. As, the link capacity limit is not sufficient it is not possible. Thus, the access point of the system should be protected from earlier.

Asymmetric data rate: The clasping time between a request message and a response message may extend from milliseconds to hours.

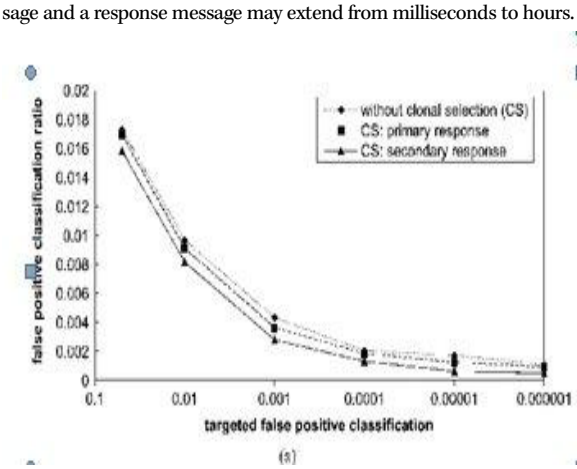

Figure.3: Performance evaluation of misbehavior detection

Volume : 4 | Issue : 3 | March 2015 • ISSN No 2277 - 8179

CONCLUSIONS

An anticipated delinquency detection scheme adopts the Inspection Game. A game theoretical analysis demonstrates the cost of delinquency detection which could be significantly reduced without compromising the detection performance. On Discussion of correlating a user's reputation of trust level to the detecting anticipation, that is expected to reduce the detecting anticipation. Detailed analysis is used to demonstrate the effectiveness and the efficiency of the iTrust.

REFERENCE

[1] Sichitiu and M. Kihl, "Inter-Vehicle Comm unication Systems: A Survey," IEEE Comm. Surveys and Tutorials, vol. 10, no. 2, pp. 88- 105, May-Aug. 2008. | | [2] U. Lee, J. Lee, J. Park, E. Amir, and M. Gerla, "FleaNet: A Virtual Market Place on Vehicular Net works," Proc. Third Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services, pp. 1-8, July | 2006. | | [3] M. Sun, W. Feng, T. Lai, K. Yamada, H. Okada, and K. Fujimura, "GPS-Based Message Broad cast for Adaptive Inter-Vehicle Communications," Proc. 52nd IEEE Vehicular Technology Conf. (VTC '00), vol. 6, pp. 2685-26 92, 2000. | | [4] S. Biswas, R. Tatchikou, and F. Dion, " Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety," IEEE Comm. Magazine, vol. 44 , no. 1, pp. 74-82,Jan. 2006. | | [5] O. Tonguz, N. Wisitpongphan, F. Bai, P. M udalige, and V. Sadekar, "Broadcasting in VANET," Procc. Mobile Networking for Vehicular Environments, pp. 7-12, May 2007. | | | [6] G. Korkmaz, E. Ekici, F. Ozguner, and U. Ozguner, "Urban MultiHop Broadcast Protocol for Inter -Vehicle Communication Systems," Proc. First ACM Int'l Workshop Vehicular Ad Hoc Networks (VANET '04), pp. 76-85, Oct. 2 004. | | | [7] G. Korkmaz, E. Ekici, and F. Ozguner, An Efficient Fully Ad-Hoc Multi-Hop Broadcast Prot ocol for Inter-Vehicular Communication Systems," Proc. IEEE Int'l Con f. Comm. (ICC '06), June 2006. |