International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 9: September 2015, pp 15-17. www.aetsjournal.com ISSN (Online) : 2394-6237

A Survey on Cluster Based Sufficient and Necessary Set Scheme for Misbehavior Detection in Adversary Environment

Kanagarohini.V, Ramya.K

Abstract— Malicious nodes directly threaten the robustness of the network as well as the availability of nodes. Protecting legitimate nodes from malicious attacks must be considered in Delay Tolerant Network (DTN) . This is achievable through the use of a key management scheme which serves as a means of conveying trust in a public key infrastructure. These certificates are signed by the Certificate Authority (CA) of the network, which is a trusted third party that is responsible for issuing and revoking certificates. An attacker's certificate can be successfully revoked by the CA if there are enough accusations showing that it is an attacker. In Existing system, the detection of malicious nodes takes high the verification time and cost and it takes more time to reach its destination. we proposed, location based routing protocol and necessary and sufficient set based scheme to reduce the verification time and cost. These algorithms exploit individual and combined strengths of sufficient and necessary sets in query processing. The extensive analysis and simulation results demonstrate the latency, total cost and throughput.

Keywords— Delay Tolerant Networks,Certificate Authority, Necessary and Sufficient Set Based Scheme.

I. INTRODUCTION

Delay Tolerant Network is a communication network designed to tolerate long delays and outages. The currentnetworking technology depends on a set of basic assumptions that are not true in all environments. The first and most important assumption is that an end-to-end connection exists from the source to the destination. This assumption can be easily contravened due to mobility, power saving etc. Examples of such networks are sensor networks with scheduled infrequent connectivity, vehicular DTNs that publish local ads, traffic reports, parking information. Delay tolerant network (DTN) is an attempt to extend the reach of networks. It give an assurance to enable communication between "challenged" networks.

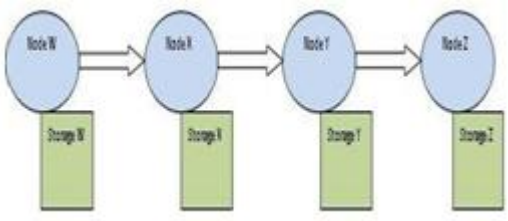


Fig. 1 Delay Tolerant Network

Kanagarohini.V, PG Scholar, SreeSowdambika College of Engineering, Tamilnadu, India. (Email: rohini.cse01@gmail.com)
Ramya.K, Assistant Professor, SreeSowdambika College of Engineering. Tamilnadu, India. (Email: sri.ramya531@gmail.com)

Delay Tolerant Networks have unique characteristics like lack of contemporaneous path, short range contact high variation in network conditions, difficult to predict mobility patterns and long feedback delay. Because of these unique characteristics the Delay Tolerant Networks (DTNs) move to an approach known as "store-carry-and-forward" strategy where the bundles can be sent over the existing link and buffered at the next hop until the next link in the path appears and the routing is determined in an "opportunistic" fashion.

Delay Tolerant Networks have unique based misbehavior detection scheme characteristics like lack of contemporaneous unsuitable for DTNs. path, short range contact high variation in Recently, there are quite a few network conditions, difficult to predict proposals for misbehaviors detection inmobility patterns and long feed back delay.DTNs most of which are based on Because of these unique characteristics the forwarding History verification (e.g.,Delay Tolerant Networks (DTNs) move to an multilayered credit, three-hop feedback approach known as "store-carry-and-mechanism, or encounter ticket which are

forward" strategy where the bundles can becostly in terms of transmission overhead andsent over the existing link and buffered at theverification cost. Further, even from thenext hop until the next link in the path

Trusted Authority (TA) point of view,appears and the routing is determined in anmisbehavior detection in DTNs inevitably"opportunistic" fashion.incurs a high inspection overhead, whichIn DTNs a node could misbehave by includes the cost of collecting the forwarding refusing to forward the packets, dropping the

history evidence via deployed judge nodespackets even when it has the potential toand transmission cost to TA. Therefore, anforward (e.g., sufficient memory and meetingefficient and adaptive misbehavior detection

opportunities) or modifying the packets toand reputation management scheme is highlylaunch attacks. These types of maliciousdesirable in DTN.behaviors are caused by rational or malicious

II. RELATED WORKS

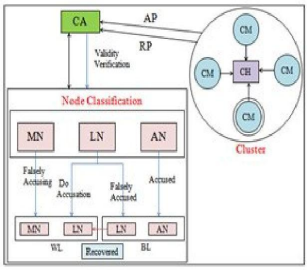
A dispersed uncertain database is reportedMitigating routing misbehavior has beenonly support top-k queries with the expectedwell studied in traditional mobile ad hocranking semantic. On the divergent, ournetworks. These works use neighborhoodsuggestion is a general approach which ismonitoring

or destination acknowledgementappropriate to

probabilistic top-k queriesto detect packet dropping , and exploit credit-with any semantic. Moreover, instead ofbased and reputation based incentive frequently requesting data which may last for schemes to stimulate rational nodes orseveral rounds our protocols are definite torevocation schemes to revoke maliciousbe completed within no more than two nodes , Even though the existing misbehavior rounds. Probabilistic ranked queries based on detection schemes work well for the uncertainty at threat tribute level are studied. Traditional wireless networks, the uniqueA unique study that ranks tuples by their network characteristics including lack of probabilities gratifying the query is contemporaneous path, high variation inpresented.

III. CLUSTER BASED ROUTINGPROTOCOL (CBRP)

Clustering is the method of grouping the)nodes present in the DTN. Due to clusterDue of the limited transmission range offormation it is easy to exchange informationwireless network, multiple "hops" are neededbetween the interacting nodes. There can beto exchange data across the network. In ordermore than one cluster and these clusters areto facilitate communication within thecommunicated with each other. Network, a routing protocol is used toNodes within this cluster are called asdiscover routes between nodes. The primaryCluster Members (CM). Every cluster willgoal of such an ad hoc network routing have Cluster Members (CMs) and a Clusterprotocol is efficient route establishmentHead (CH). Cluster Heads are the backbonebetween a pair of nodes so that messagesfor communication in the network. Cluster may be delivered in a timely manner.



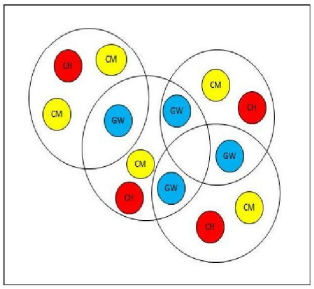


Fig. 2 shows that there is availability of Custer Heads(CHs) in each cluster, which maintains the information of other nodes. Gateway nodes are also present in a clusters. Where,CH= Cluster Head, CM= Cluster Member, GW= Gateway Node.

Where,
AN = Attacker Node, AP = Accusation Packet, BL = Black List,
CM with double circle = Accused Node,
MN = Malicious Node,
LN = Legitimate Node,
RP = Recovery Packet, WL = Warning List.

Path finding will be as follows. First a Source(s) nodes hello mess to its cluster head (ch), attached with a destination name. If the destination comes under current ch means, it will forward hello to that destination with source name. Else if destination not in its region means, it simply forward the message to next cluster head through the gate way.

And this process will be continued still destination found or still reaching mess to all cluster heads. Once if destination receives the message then it will replay for that message in the path and starts path minimizing also. First it checks that its neighbors were present or not. If not it forwards message to the previous node. If its there means it will delete the nodes in the path between those two nodes (if any nodes were present) and the message is forwarded to its previous node in new (minimized) path. And this process takes place till message reaches the source. And the message transferred through this path.

IV. SUFFICIENT AND NECESSARYSET BASED SCHEME

Response time is one more significant metrics to assess query processing algorithms in wireless networks. All of those Two algorithms like SSB, NSB execute at most two rounds of message swap there is not much difference among SSB, NSB in terms of query response time. Thus, we focus on the verification time and data transmission cost in the valuation. An intuitive way for in-network data processing is to transmit the sufficient set to base station. The tuples not included in the sufficient set neither have top-k probability higher than p nor affect the top-k probability of qualified tuples in the final answer. Consequently, the SSB algorithm consists of only one communication phase from cluster heads to the base station. After collecting data tuples from its cluster, a cluster head computes the sufficient set from the local collected tuples and sends it to the base station. Note that if a sufficient set cannot be obtained, all the local data tuples are transmitted. After receiving the transmitted data tuples from all the cluster heads, the base station computes the query answer by a centralized algorithm.

The necessary set contains only 1) locally qualified tuples that have local top-kprobability higher than p and 2) supplementary tuples ranked higher than those in (1) (Because they are needed to compute top-k probabilities of these qualified tuples). However, even though all the tuples that potentially have top-k probabilities higher than p are included in the necessary set, calculating their global top-k probabilities may still need to access some additional supplementary tuples. Therefore, NSB may have two phases when these additional supplementary tuples are needed.

AT CLUSTER HEAD:

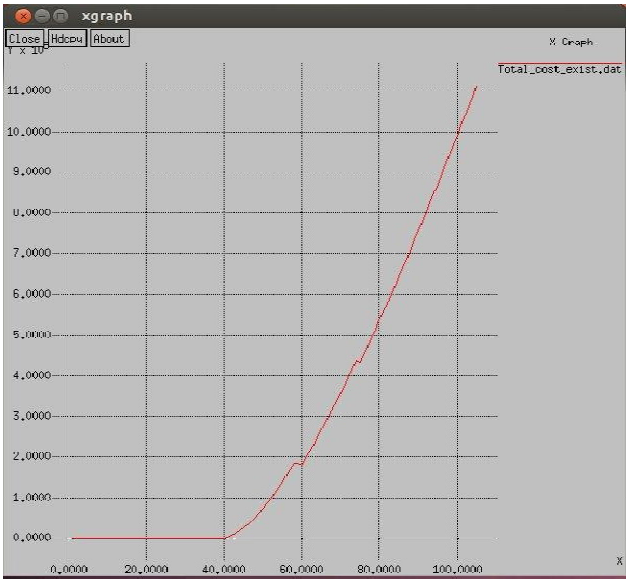
Compute the necessary boundary
$NB(Ti), N(Ti) \leftarrow \{x | x \leq f\, NB(Ti) \Lambda\, x \in Ti\}$

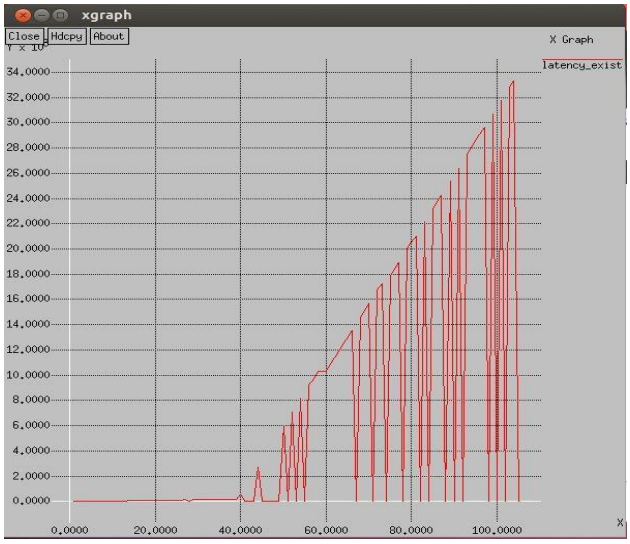
Deliver N(Ti) to the base station
if cluster head receive GB from the base station
then
N′(Ti) ←{ x|x ≤f GB Λ x Є [Ti - N(Ti)]} Now, N′(Ti) is send to the base station. end if

AT BASESTATION:

It receives the tuple N (Ti) from the cluster head.
(1 ≤ i ≤ N)
T′ ← U1 ≤ i ≤ N N(Ti)
Now, it will calculate the global boundary. if global boundary GB is less than that of NB(Ti), then
It calculate the final necessary boundary Else
It will broadcast GB to ci and once again it collects necessary tuple
T′ ← U1≤ i ≤ N N′(Ti) end if
Where, x is the tuple ci is the cluster head N(Ti) is the necessary set
NB(Ti) is the necessary boundary
Ti is the records collected from the sensor N is the number of clusters in the zone
T′ is the aggregation of data sets received from the clusters.

V. RESULT ANALYSIS





VI. CONCLUSION

In this paper we propose a cluster based necessary and sufficient set scheme to detect malicious node and ensures secure transmission of data. The selection of neighbor node is based on the location based routing protocol, by which the packet dropping rate is considerably reduced and it also simplifies the work of Trusted Authority (TA). We also reduce the Verification timeand cost by introducing the sufficient and necessary set based scheme.

REFERENCES

[1] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANETBased Smart Parking Scheme for Large Parking Lots," Proc. IEEE INFOCOM '09, Apr. 2009.
[2] 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.
[3] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay-Tolerant Networks," Proc. IEEE INFOCOM '10, 2010.
[4] 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.
[5] 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.
[6]P.Vinuthna,, T.SaiDurga, "Network Processing of PT-TOPK Queries Using Necessary Set Based Algorithm in WSN's" International Journal of Research in Computer and Communication Technology, Vol 3, Issue 10, October – 2014.
[7] Sujithra.M, Gokulakrishnan.V, "An Adaptive Algorithm for Distributed Processing in Multidimensional Data Sets" International Conference on Engineering Technology and Science On 10 February 2014.
[8] M. Hua, J. Pei, W. Zhang, and X. Lin, "Ranking Queries on Uncertain Data: A Probabilistic Threshold Approach," Proc. ACMSIGMOD Int'l Conf. Management of Data (SIGMOD '08), 2008.