An Efficient Intrusion Detection Scheme for Mitigating Nodes Using Data Aggregation in Delay Tolerant Network

A.S.Syed Navaz, J.Antony Daniel Rex, P.Anjala Mary

Abstract— Delay tolerant networks (DTNs) exploit the intermittent connectivity between mobile nodes to transfer data. Due to a lack of consistent connectivity, two nodes exchange data only when they move into the transmission range of nodes In DTNs, a node may misbehave by dropping packets even when it has sufficient buffers. Routing misbehavior can be caused by selfish nodes that are unwilling to spend resources such as power and buffer on forwarding packets of others, or caused by malicious nodes that drop packets to launch attacks To address the problem, we recommend a distributed scheme to detect packet dropping in DTNs. In planned TP Trust misbehavior detection scheme, is required to keep a signed contact records of its previous contacts of transfer data, disseminated to a certain number of witness nodes, carry and store which can collect appropriate contact records and detect the misbehaving nodes to resend analysis with NDD. We also planned a scheme to mitigate routing misbehavior by limiting the number of packets forwarded to the misbehaving nodes. Trace-driven simulations show MASP to transfer the data with secure group aggregators to give security to our solutions are efficient and can effectively mitigate routing misbehavior.

Index Terms— DTN, Network, Nodes, Clustering, Detection, Cryptography. TCP/IP.

1 INTRODUCTION

Most popular Internet applications rely on the existence of a contemporaneous end-to-end link between the source and the destination, with moderate round-trip times and small packet loss probabilities. This fundamental assumption is not expected in some challenged networks, which are often referred to as delay-tolerant networks (DTNs). Applications of this emergent communication paradigm are wide ranging and include low-cost Internet service provision in remote or developing localities vehicular DTNs for dissemination of location-dependent information (e.g., local ads, traffic reports, and parking information) or for providing multichip Internet access social-based networks to allow humans to communicate without network infrastructure pockets witched networks underwater networks etc. In DTNs, the in-transit messages, which are also called 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 node wakes up). This message propagation process is usually referred to as the "store-carry-and-forward" strategy, and routing is made in an "opportunistic" fashion.

Previously reported studies have focused on opportunistic data propagation in DTNs which depends on the hypothesis that each individual node is ready to forward packets for others. This hypothesis, however, might easily be violated in the presence of selfish or even malicious nodes, which may choose to save their precious wireless resources by refusing to serve as bundle relays Such selfishness actions may be more challenging for researchers in certain applications of DTNs such as vehicular DTNs and social networks, which are decentralized and distributed over a multitude of devices that are controlled and operated by individuals. In these applications, it is highly possible that there exist some selfish users who may not want to forward such bundles without compensation. Furthermore, even from the security point of view, naive packet forwarding may open a new door for malicious users, who may intentionally try to launch denial-of-service attacks on the network by flooding the network with dummy messages. Thus, to deploy an applicable DTN in real-world scenarios, proper incentives and security mechanisms should be in place.

It is a networking architecture that is designed to provide communications in the most unstable and stressed environments, where the network would normally be subject to frequent and long lasting disruptions and high bit error rates that could severely degrade normal communications.DTN works using different kind of approach than TCP/IP for packet delivery that is more resilient to disruption than TCP/IP. DTN is based on a new experimental protocol called the Bundle Protocol (RFC 5050). BP sits at the application layer of some number of constituent internets, forming a store-and-forward overlay network. The Bundle Protocol (BP) operates as an overlay protocol that links together multiple subnets into a single network. The basic idea behind DTN network is that endpoints aren't always continuously connect-

A.S.SYED NAVAZ *working as an Assistant Professor in the Department of Computer Science at Muthayammal College of Arts & Science, Namakkal, India E-Mail: a.s.syednawaz@gmail.com,*

:

J.ANTONY DANIEL REX *working as an Assistant Professor in the Department of Computer Science at St. Joseph's College of Arts & Science (Autonomous), Cuddalore, India.*

P.ANJALA MARY, *working as an Assistant Professor in the Department of Computer Science at St. Joseph's College of Arts & Science (Autonomous), Cuddalore, India*

ed. In order to facilitate data transfer, DTN uses a store-and-forward approach across routers that are more disruption-tolerant than TCP/IP. However, the DTN approach doesn't necessarily mean that all DTN routers on a network would require large storage capacity in order to maintain end-to-end data integrity. Disruption Tolerant Networks are frequently used in disaster relief missions, peace-keeping missions, and in vehicular networks. Most recently NASA has tested DTN technology for spacecraft communications. A disruption-tolerant network (DTN) is a network designed so that temporary or intermittent communications problems, limitations and anomalies have the least possible adverse impact. Disruption-tolerant networks (DTNs) provide communication in scenarios that challenge traditional mobile network solutions. DTNs use the inherent mobility of the network to deliver messages in the face of sparse deployments, highly mobile systems, and intermittent power. DTN routing differs from previous networking paradigms by assuming that connectivity will be unpredictable and poor, so information must be opportunistically routed toward the final destination. In addition to those challenges, malicious adversaries may threaten connectivity in a DTN by inserting, flooding, corrupting, and dropping messages. In traditional, infrastructure based networks and mantes, security is often provided by restricting participation to a specific set of authorized nodes, enforced with cryptographic keys and identity management. In such a system, an administrator certifies all nodes in the network and participants will only route messages through other authorized nodes. The routing protocol used in a DTN strongly influences the security properties of the system. Two characteristics in routing protocols are : criterion and style. The criterion refers to the process by which neighboring nodes are passed packets; specifically, metric based and random criteria. The style indicates whether the protocol is explicative or forwarding.

Routing misbehavior 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. The recent researches show that routing misbehavior will significantly reduce the packet delivery rate and thus pose a serious threat against the network performance of DTN, Therefore, a misbehavior detection and mitigation protocol is highly desirable to assure the secure DTN routing as well as the establishment of the trust among DTN nodes in DTNs. Mitigating routing misbehavior has been well studied in traditional mobile ad hoc networks. These works use neigh boyhood monitoring or destination acknowledgement to detect packet dropping, and exploit credit-based and reputation- based incentive schemes to stimulate rational nodes or revocation schemes to revoke malicious nodes. Even though the existing misbehavior detection schemes work well for the traditional wireless networks, the unique network characteristics including lack of contemporaneous path, high variation in network conditions, difficult to predict mobility patterns, and long feedback delay, have made the neighborhood monitoring based misbehavior detection scheme unsuitable for DTNs.

A launches the black hole attack by refusing to forward the packets to the next hop receiver C. Since there may be no neighboring nodes at the moment that B meets C, the misbehavior (e.g., dropping messages) cannot be detected due to lack of witness, which renders the monitoring based misbehavior detection less practical in a sparse DTN. In specific, SMART is based on the notion of a layered coin that provides virtual electronic credits to charge for and reward the provision of data forwarding in DTNs. Such coin is composed of multiple layers, each of which is generated by the source/destination or an intermediate node. The first layer, which is also named the base layer, is generated by the source to indicate the payment rate (credit value), remuneration conditions, and the class-of-service (CoS) requirement and other reward policies. During the subsequent bundle propagation process, each intermediate node will generate a new layer based on the previous layers by appending a no forgeable digital signature. This new layer is also called the endorsed layer, which implies that the forwarding node agrees to provide forwarding service under the predefined CoS requirement and will be rewarded according to the reward policy in the future. With endorsed layers, it is easy to track the propagation path and determine each intermediate node by checking the signature of each endorsed layer. In the rewarding and charging phase, if the provided forwarding service satisfies remuneration conditions defined in the predefined reward policy, each forwarding node along one or multiple path(s) will share the credit defined in this coin depending on different data-forwarding algorithms (single-copy/multicopying forwarding) and the actual forwarding results (bundle delivered along one or multiple paths).

However, the main challenge in designing SMART is to ensure that the security properties of the scheme are not compromised. Since all security related to a coin, particularly during the store-carry-and-forward process, is managed by the intermediate nodes, a selfish node (or even a group of colluding nodes) may attempt to cheat the system to maximize its expected welfare. As an example, a selfish node may arbitrarily inject a fake layer into the current coin or remove several valid layers from it, if such actions can maximize its welfare. This is the security perspective of SMART. Second, any security functionality will incur extra computation and transmission overhead. A secure credit-based incentive scheme should be efficient enough to not significantly compromise the system performance. This is the performance perspective of our system. The contributions of this paper can be summarized as

follows: First, we planned a SMART scheme to stimulate cooperation among selfish nodes in DTNs. The plannedd scheme can be made compatible with diverse data-forwarding algorithms in DTNs. Second, SMART can withstand a wide range of cheating actions because of its novel layer concatenation technique.

Delay Tolerant Networks (DTNs) have the unique feature of intermittent connectivity, which makes routing uite different from other wireless networks. For example, since an end-to-end connection is hard to setup, store-carry and forward is used to deliver the packets to the destination. Although many routing algorithms have been plannedd to increase data delivery reliability, they are purely based on contact opportunity; i.e., they are designed without considering users' willingness and implicitly assume that all nodes are willing to forward packets for others.

In the real world, most people are selfish. As a result, in civilian DTNs such as PeopleNet and Pocket Switched Network a node may not be willing to forward packts for others. Then, previous algorithms may not work well since some packets are forwarded to nodes unwilling to relay, and will be dropped. Although many researchers have designed incentive schemes to stimulate selfish nodes to forward packets in mobile ad hoc networks they go to another extreme; i.e., they believe that users are selfish and are not willing to forward packets for anyone else. To capture user selfishness in a more realistic manner, we have two observations from the social perspective. First, a selfish user is usually willing to help others with whom he has social ties (e.g., friends, coworkers, roommates), because he got help from them in the past or will probably get help from them in the future. In this paper, a social tie means an interpersonal tie that falls into the strong or weak category defined in Second, for those with social ties, a selfish user may give different preferences. That is, he is willing to provide better service to those with stronger ties than those with weaker ties, especially when there are resource constraints. For easier presentation and comparison, such refined selfishness model will be referred to as social selfishness and the previously well studied simple model is called individual selfishness. Social selfishness is not totally contradictory to individual selfishness, but is a generic extension to it. When a node has no social tie to the outside world, his social selfishness becomes individual selfishness.

1.1 Metric-based DTN routing protocols

DTNs attempt to route packets via intermittently connected nodes. Most of the previous work on DTNs has been based on various assumptions regarding connectivity and the availability of environmental knowledge and control. Some of them even assume that nodes know all future contact information. Since the real mobility trace the recent experimental DTNs appear to be cyclic to a large extent, several recently-plannedd routing protocols in DTNs designed metrics to summarize the information of contact history. These metric-based DTN routing protocols use history to predict the future and are widely applicable. However, all of them assume the truthfulness of the history information and omit the possibility of attacks by providing faked metrics.

2. Related Work

Credit-based incentive schemes introduce some form of virtual currency to regulate the packet-forwarding relationships among different nodes. There are two different ways to realize such kind of credits: 1) game-theory-based schemes and 2) security-protocol-based schemes. The first approach tries to investigate such no cooperative communication scenarios within a game theory framework whereas the second approach focuses on ensuring the security of the credits by using various cryptographic tools Most of these schemes always assume that an end-to-end path exists and is determined before the data-forwarding process. However, this assumption obviously does not hold in DTNs, which makes them not suitable in DTNs. In a virtual-cash based incentive scheme is plannedd to stimulate commercial advertisement dissemination in vehicular networks. In it is suggested to use a multilevel coupon-based scheme to stimulate exchanging information about places of interest or local restaurants. However, in both schemes, the focus is on how to stimulate advertisement dissemination, and transmission is based on simple broadcasting, whereas DTN routing is not taken into consideration.

2.1 Literature Survey

KNOW THY NEIGHBOR: TOWARDS OPTIMAL MAPPING OF CONTACTS TO SOCIAL GRAPHS FOR DTN ROUTING, THEUS HAUSSMANN, THRASYVOULOS SPYROPOULOS, AND FRANCK LEGENDRE.

Delay Tolerant Networks (DTN) are networks of self-organizing wireless nodes, where end-to-end connectivity is intermittent. In these networks, forwarding decisions are generally made using locally collected knowledge about node behavior (e.g., past contacts between nodes) to predict future contact opportunities. The use of complex network analysis has been recently suggested to perform this prediction task and improve the performance of DTN routing. Contacts seen in the past are aggregated to a social graph, and a variety of metrics (e.g., centrality and similarity) or algorithms (e.g., community detection) have been plannedd to assess the utility of a node to deliver content or bring it closer to the destination. In this paper, we argue that it is not so much the choice or sophistication of social metrics and algorithms that bears the

most weight on performance, but rather the mapping from the mobility process generating contacts to the aggregated social graph. We first study two well-known DTN routing algorithms Sims Bet and Bubble Rap that rely on such complex network analysis, and show that their performance heavily depends on how the mapping (contact aggregation) is performed. What is more, for a range of synthetic mobility models and real traces, we show that improved performances (up to a factor of 4 in terms of delivery ratio) are consistently achieved for a relatively narrow range of aggregation levels only, where the aggregated graph most closely reflects the underlying mobility structure. To this end, we planned an online algorithm that uses concepts from unsupervised learning and spectral graph theory to infer this "correct" graph structure; this algorithm allows each node to locally identify and adjust to the optimal operating point, and achieves good performance in all scenarios considered. To combat the inherent uncertainty of future contact opportunities, many protocols forward in parallel multiple replicas of the same content or resort to coding (network coding, erasure coding). Nevertheless, node mobility (and resulting contact opportunities) are not entirely random. Instead, weak or strong patterns are present. To this end, numerous utility based routing schemes attempt to differentiate nodes that are more likely to deliver content or bring it closer to the destination. Among them, a number of schemes implicitly assess the strength of ("social") ties between nodes. For example uses time of last encounter, and [9] uses contact frequency as a hint on the similarity of mobility patterns. use instead a metric much akin to degree centrality to identify nodes that are highly mobile/social; the former scheme is reminiscent of search in scale-free networks, while the latter uses centrality to choose which relays to "spray" a limited budget of message replicas to. However, these simple metrics may only capture one facet of the underlying mobility process, which can hinder good contact predictions.

Complex network analysis (CNA) has recently been planned as a more generic and powerful tool to formulate and solve the problem of future contact prediction in DTNs. Past observed contacts between nodes are aggregated into a social graph, with graph edges representing (one or more) past meetings between the vertices. An edge in this graph conveys the information that two nodes often encounter each other either because they have a strong social tie (friends), or because they are frequently co-located without actually knowing each other (familiar strangers); thus, existence of an edge intends to have predictive capacity for future contacts.

ROUTING IN SOCIALLY SELFISH DELAY TOLERANT NETWORKS, QINGHUA LI, SENCUN ZHU, GUOHONG CAO

Offered routing algorithms for Delay Tolerant Networks (DTNs) assume that nodes are willing to forward packets for others. In the real world, however, most people are socially selfish; i.e., they are willing to forward packets for nodes with whom they have social ties but not others, and such willingness varies with the strength of the social tie. Following the philosophy of design for user, we planned a Social Selfishness Aware Routing (SSAR) algorithm to allow user selfishness and provide better routing performance in an efficient way. To select a forwarding node, SSAR considers both users' willingness to forward and their contact opportunity, resulting in a better forwarding strategy than purely contact-based approaches. Moreover, SSAR formulates the data forwarding process as a Multiple Knapsack Problem with Assignment Restrictions (MKPAR) to satisfy user demands for selfishness and performance. Trace-driven simulations show that SSAR allows users to maintain selfishness and achieves better routing performance with low transmission cost have two observations from the social perspective. Such refined selfishness model will be referred to as social selfishness and the previously well studied simple model is called individual selfishness. Social selfishness is not totally contradictory to individual selfishness, but is a generic extension to it. When a node has no social tie to the outside world, his social selfishness becomes individual selfishness. However, in most cases, social selfishness conveys more meaning. allow users to behave as what their social selfishness requires, but try to improve the routing performance under the social selfish behavior. Our underlying philosophy is that social selfishness is a kind of user demand that should be satisfied. It should be treated as a design metric to measure the user satisfaction, similar to other traditional performance metrics such as data delivery ratio and delay. We call such design philosophy "design for user".

Social selfishness will affect node behaviors. As a forwarding service provider, a node will not forward packets received from those with whom it has no social ties, and it gives preference to packets received from nodes with stronger ties when the resource is limited. Thus, a DTN routing algorithm should take the social selfishness into consideration. In DTNs, nodes have limited bandwidth and computational capability. As in other studies, we assume each node has unlimited buffer for its own packets, but limited buffer for others. As for data traffic, we only consider uncast, and assume each packet has a certain lifetime (i.e., TTL). We further assume bidirectional links, which can be provided by some MAC layer protocols, e.g., IEEE 802.11.

Trust Model We assumes the source of a packet is anonymous to intermediate nodes. For example, the source ID can be encrypted in a way so that only the destination can decrypt. Then intermediate nodes provide data forwarding service only based on the previous hop information. This assumption is not essential to SSAR, and we add it just to simplify the routing model. We also assume that some authentication service is

available so that one node can not impersonate another. Otherwise, a node may claim to be someone else to obtain forwarding services from that node's social ties. How to provide such authentication service has been well studied and is out of the scope of this paper. Adversary Model In this paper, we only consider socially selfish behaviors. Malicious attacks (e.g., DOS, wormhole, black hole) and free-riding behaviors are not our focus. This is not because we do not think they are important, but because we believe they deserve separate studies.

A RESERVATION-BASED SMART PARKING SYSTEM, HONGWEI WANGAND WENBO HEY

Finding a parking space in most metropolitan areas, especially during the rush hours, is difficult for drivers. The difficulty arises from not knowing where the available spaces may be at that time; even if known, many vehicles may pursue very limited parking spaces to cause serious traffic congestion. In this paper, we design and implement a prototype of Reservation-based Smart Parking System (RSPS) that allows drivers to effectively find and reserve the vacant parking spaces. By periodically learning the parking status from the sensor networks deployed in parking lots, the reservation service is affected by the change of physical parking status. The drivers are allowed to access this cyber-physical system with their personal communication devices. Furthermore, we study state-of-the-art parking policies in smart parking systems and compare their performance. The experiment results show that the planned reservation-based parking policy has the potential to simplify the operations of parking systems, as well as alleviate traffic congestion caused by parking searching.

For instance, a recent survey shows that during rush hours in most big cities, the traffic generated by cars searching for parking spaces takes up to 40% of the total traffic. To alleviate such traffic congestion and improve the convenience for drivers, many smart parking systems aiming to satisfy the involved parties (e.g., parking service providers and drivers) have been deployed. The current smart parking or parking guidance systems only obtain the availability information of parking spaces from deployed sensor networks, and simply publish the parking information to direct drivers. However, since these systems cannot guide the drivers to their desired parking destinations, even sometimes make the situation worse, they are not "smart" enough. For instance, when the number of vacant spaces in an area is limited, more drivers, who obtain the parking information, are heading for these spaces. It will cause severer congestion. It is, therefore, strongly desired to provide an effective strategy to address these concerns.

SELF RECOGNITION OF ROUTING MISBEHAVIOUR IN DISRUPTION TOLERANT NETWORKS, K.PRASANTH KUMAR, S.OVIYA, J.RAJASEKAR, S.SATHISH KUMAR

A Disruption tolerant networks is a network designed temporary, have the unique features of intermittent connectivity which makes routing quite different from other wireless network. Routing misbehavior like selfish or malicious node can cause packet delay and modifying packets in a network. A node is required to keep a few signed contact record of its previous contact based on it the next node can detect a packet dropping, although here it may reduces the packet delivery ratio and waste the system resources such as power and bandwidth. To reduce this problem we planned a scheme as record handler, it is used to maintain the entire information about packet separately and to provide more security and we introduce RC4 algorithm where the message and the key can be send individual to nodes for avoiding misbehavior on a network. Fault-tolerant systems are designed so that if a component fails or a network route becomes unusable, a backup component, procedure or route can immediately take its place without loss of service. At the software level, an interface allows the administrator to continuously monitor network traffic at multiple points and locate problems immediately. In hardware, fault tolerance is achieved by component and subsystem redundancy. Graceful degradation has always been important in large networks. One of the original motivations for the development of the Internet by the Advanced Research Papers Agency (ARPA) of the U.S. government was the desire for a large-scale communications network that could resist massive physical as well as electronic attacks including global nuclear war. In graceful degradation, a network or system continues working to some extent even when a large portion of it has been destroyed or rendered inoperative. Electronic attacks on networks can take the form of viruses, worms, Trojans, spyware and other destructive programs or code. Other common schemes include denial of service attacks and malicious transmission of bulk e-mail or spam with the intent of overwhelming network servers. In some instances, malicious hackers commit acts of identity theft against individual subscribers or groups of subscribers in an attempt to discourage network use. In a DTN, such attacks may not be entirely preventable but their effects are minimized and problems are quickly resolved when they occur. Servers can be provided with antivirus software and individual computers in the system can be protected by programs that detect and remove spyware. As networks evolve and their usage levels vary, routes can change, sometimes within seconds. This can cause temporary propagation delays and unacceptable latency. In some cases, data transmission is blocked altogether. Internet users may notice this as periods during which some Web sites take a long time to download or do not appear at all. In a DTN, the frequency of events of this sort is kept to a minimum. Routing is the transfer of data packets from one location to another, and it's one of the fundamental network functions. Network throughput, which is the ratio of data packets sent and received, is directly related to the routing function of any net-

work. In other words, if the routing function is good enough, then we can expect a better output from the network. In today's environment, we see different types of networks.

3. EXISTING SYSTEM

Malicious and selfish behaviors represent a serious threat against routing in delay/Delay tolerant networks (DTNs). Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge. In this paper, we planned ITRUST, a probabilistic misbehavior detection scheme, for secure DTN routing toward efficient trust establishment. The basic idea of ITRUST is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. The prior model ITRUST as the inspection game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost. To further improve the efficiency of the planned scheme, we correlate detection probability with a node's reputation, which allows a dynamic detection probability determined by the trust of the users.

3.1 Disadvantages

- Destination gets the wrong information from hackers or malicious user.
- There is no any server to detect hackers.
- Overhead of packet loss
- Low level network performance.

4. PROPOSED SYSTEM

Delay Tolerant Networks (DTNs) have the unique feature of intermittent connectivity, which makes routing quite different from other wireless networks. Since an end-to-end connection is hard to setup, store-carry-and-forward is used to deliver the packets to the destination. The planned system forms clusters among the nodes in the DTN with Neighbors distance discovery (NDD). Clustering of nodes has various advantages. The components of a cluster are usually connected to each other through fast area networks, with each node (computer used as a server) running its own instance of an operating system. In the planned system carry to store and sent data approach the nodes in the network are clustered aiming at traffic reduction, reduction on the energy consumption by the nodes in the network and to reduce the time taken to detect the malicious node in the network. We address routing misbehavior in DTNs to detect packet dropping and to transfer maximum amount shortest path protocol to limit the traffic flowing to the misbehaving nodes. Also provide group aggregations to secure the data transfer Forwarding the history information to detect the misbehaviors' in the network is also found to be inefficient as it will require more security due to the exposure of preceding information .

4.1 Advantage

- To reduce the packet delay and detect the attacker
- Improve the network performance
- Data delivery quickly from source to destination
- Efficient data transmission on network
- Without any loss data will be send in destination

5. MODULES

5.1 Maximum Amount Shortest Path Algorithm

Each node attempts to route packets to their destinations over paths of minimum distance and updates the distances periodically to adapt topological and traffic changes.

- distance-vector
- Link-state.

5.2 Distance-vector

Each node maintains a routing table containing the distance of the shortest path to every destination in the network. A node only informs its immediate neighbors of distance discovery.

5.3 Link state

Each node can route packets to a particular, destination calculating the shortest path form itself to the destination node.

5.4 SHORTEST PATH ROUTING

A path between two nodes may go through several intermediary nodes and arc. To find a path between two nodes that has the smallest total cost where the total cost of a path is the sum of the arcs cost in that path.

5.5 MISBEHAVIORING NODES

Every node in the network maintains a rating for its entire neighbor node. Then path metric is calculated by taking the mean of all the rating values. Negative metric value is assigned to nodes that are detected to misbehave and thus it is avoided in the path selection. Shortest path is selected to transfer packet through the network.

5.6 MISBEHAVORING NODE IS DETECTED BY DTN

Misbehaving nodes may falsify some records to avoid being detected, but this will violate some consistency rules. To detect such inconsistency, communication report is collected by contact node and detects the misbehaving nodes with certain probability. A scheme to mitigate routing misbehavior by converting the misbehavior node to legitimate node is done. The misbehaving nodes reduce the packet delivery ratio and wastes system resources such as power and buffer. Such misbehaving nodes are converted to legitimate nodes. This increases the availability of the network.

5.7 PACKETS DROPPING DETECTION

In DTN routing misbehavior is reduced by identifying malicious node using packets dropping detection. The packets drop naturally happen in the network. By comparing the buffer level of every node and assigning bandwidth as per the category in DTN Genuine traffic packet loss is differentiated with malicious packet loss. To find the capacity of the node buffer a technique called Buffer Capacity Technique is used. Even though the node has a required buffer capacity, sometimes packets drop occurs in the network. It is called malicious packet loss. A packet loss is said to be genuine packet loss if the node does not have require buffer capacity to transfer the data or due to buffer overflow.

5.8 END TO END DELAY OF DTN

The end to end processing delay is the time that a node spends processing a packet. This includes times for error checking, time includes time for error checking, time for reading the packet header, and time for looking up the link to the next node, based on the destination address.

5.9 CLUSTERING WITH NODES CONNECTIVITY

All nodes in the same square together form a cluster. This method needs node coordinates, and the graph instances used for testing indeed contain this information. However, this is the only point where they are used. The idea is to define structuraldescriptorofclustersonthegraphandtoassumethatt-woclustershave large affinity if the ir structural descriptors undergo substantial change when merging the min to one cluster. Akeyinsightofthispapertotreataclusterasadynamicalsystemanditssamplesasstates.Based on that, Path Integral, whichhasbeenintroducedinstatisticalmechanicsandquantummechanics,is utilized to measure the stability of a dynamical system.

6. CONCLUSION

We concluded that to Routing misbehavior can be caused by selfish nodes that are unwilling to spend resources such as power and buffer on forwarding packets of others, or caused by malicious nodes that drop packets to launch attacks. A scheme to mitigate routing misbehavior by limiting the number of packets forwarded to the misbehaving nodes. Trace-driven simulations show MASP to transfer the data with secure group aggregators to give security to our solutions are efficient and can effectively mitigate routing misbehavior.

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] 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.

[7] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom '00, 2000.

[8] 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.

[9] F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM '09, 2009.

[10] E. Ayday, H. Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay-Tolerant Networks," Proc. Military Comm. Conf. (Milcom '10), 2010.

[11] D. Fudenberg and J. Tirole, Game Theory. MIT Press, 1991.

[12] M. Rayay, M.H. Manshaeiy, M. Flegyhziz, and J. Hubauxy, "Revocation Games in Ephemeral Networks," Proc. 15th ACM Conf. Computer and Comm. Security (CCS '08), 2008.

[13] S. Reidt, M. Srivatsa, and S. Balfe, "The Fable of the Bees: Incentivizing Robust Revocation Decision Making in Ad Hoc Networks," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), 2009.

[14] B.B. Chen and M.C. Chan, "Mobicent: A Credit-Based Incentive System for Disruption-Tolerant Network," Proc. IEEE INFOCOM '10, 2010.

[15] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM '03, 2003.

[16] J. Douceur, "The Sybil Attack," Proc. Revised Papers from the First Int'l Workshop Peer-to-Peer Systems (IPTPS '01), 2001.

[17] R. Pradiptyo, "Does Punishment Matter? A Refinement of the Inspection Game," Rev. Law and Economics, vol. 3, no. 2, pp. 197- 219, 2007.

[18] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM '06, 2006.

[19] A.S.Syed Fiaz, M. Usha and J. Akilandeswari," A Brokerage Service Model for QoS support in Inter-Cloud Environment ", International Journal of Informatics and Computation Technology Research (IJICT), Vol.3, No. 4, pp 257-260.

[20] A. Lindgren and A. Doria, "Probabilistic Routing Protocol for Intermittently Connected Networks," draft-lindgren-dtnrg-prophet- 03, 2007.

[21] W. Gao and G. Cao, "User-Centric Data Dissemination in Disruption-Tolerant Networks," Proc. IEEE INFOCOM '11, 2011.

[22] A. Keranen, J. Ott, and T. Karkkainen, "The ONE Simulator for DTN Protocol Evaluation," Proc. Second Int'l Conf. Simulation Tools and Techniques (SIMUTools '09), 2009.

AUTHOR'S BIOGRAPHY

A.S.SYED NAVAZ received M.Sc in Information Technology from K.S.Rangasamy College of Technology, Anna University, Coimbatore, M.Phil in Computer Science from Prist University, Thanjavur, M.C.A from Periyar University, Salem and Pursuing Ph.D in the area of Wireless Sensor Networks. He researched and published in International journals and working as Editorial Board Member & Reviewer for International journals also Member in 13 International Social Bodies. Currently he is working as an Assistant Professor in the Department of Computer Science at Muthayammal College of Arts & Science, Namakkal, India. His Research areas are Wireless Sensor Networks, Mobile Computing & Image Processing.

J.ANTONY DANIEL REX received M.C.A from Periyar University, Salem, M.Phil. in Computer Science from Government arts college ,Salem, He researched and published 2 International journals & Presented one paper in national conference and one paper in International conference . Currently he is working as an Assistant Professor in the Department of Computer Science at St.Joseph's College of Arts & Science (Autono-mous), Cuddalore, India. His Research areas are Wireless Sensor Networks, Mobile-Adhoc network & Image processing.

P.ANJALA MARY received M.Sc., from St.Joseph's College Of Arts and Science - Cuddalore, Thiruvalluvar University, Vellore, M.Phil in Computer Science from St.Joseph's College Of Arts and Science, Cuddalore, Thiruvalluvar University, Vellore, She presented one paper in National conference. Currently she is working as an Assistant Professor in the Department of Computer Application at St.Joseph's College of Arts & Science (Autonomous), Cuddalore, India. Her Research areas are Data mining & Image Prrocessing.