ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Special Issue 11, March 2016

A SURVEY OF TECHNIQUES USED TO DETECT THE SELFISH NODES IN VANET

V.Vidhya [1], S.Ramkumar [2]

1. P.G. Student, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India
2. Asst.Professor, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India

Abstract: **Vehicular ad-hoc networks (VANETs) assume that mobile nodes voluntary cooperate in order to work properly. This cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to selfish node behaviour. Thus, the overall network performance could be seriously affected. The use of watchdogs is a well-known mechanism to detect selfish nodes. However, the detection process performed by watchdogs can fail, generating false positives and false negatives that can induce to wrong operations. Moreover, relying on local watchdogs alone can lead to poor performance when detecting selfish nodes, in term of precision and speed. This is specially important on networks with sporadic contacts, such as delay tolerant networks (DTNs), where sometimes watchdogs lack of enough time or information to detect the selfish nodes. Thus, we propose collaborative contact-based watchdog (CoCoWa) as a collaborative approach based on the diffusion of local selfish nodes awareness when a contact occurs, so that information about selfish nodes is quickly propagated. As shown in the paper, this collaborative approach reduces the time and increases the precision when detecting selfish nodes.**

I. INTRODUCTION

Cooperative networking is currently receiving significant attention as an emerging network design strategy for future mobile wireless networks. Successful cooperative networking can prompt the development of advanced wireless networks to cost-effectively provide services and applications in contexts such as vehicular ad hoc networks (VANETs) or mobile social networks. Two of the basic technologies that are considered as the core for these types of networks are Mobile Ad-Hoc Networks (MANETs) and Routing Network (RN) Opportunistic and The cooperation on these networks is usually contact-based. Mobile nodes can directly communicate with each other if a contact occurs (that is, if they are within communication range). Supporting this cooperation is a cost intensive activity for mobile nodes. Geo caching is an outdoor recreational activity in which the participants use a Global Positioning System (GPS) receiver or mobile device and other navigational techniques to hide and seek containers, called "geo caches" or "caches", anywhere in the world. A typical cache is a small waterproof container containing a logbook where the geocach enters the date they found it and signs it with their established code name. Larger containers such as plastic storage containers (Tupperware or similar) or ammunition boxes can also contain items for trading, usually toys or trinkets of little value. Geo caching shares with benchmarking, trigpointing, orienteering, treas ure-hunting,letterboxing & way marking.Geo caches are currently placed in over 200 countries around the world and on all seven

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Special Issue 11, March 2016

continents, including Antarctica, and the International Space Station. After more than 12 years of activity there are over 1.8 million active geo caches published on various websites. There are over 5 million geocachers worldwide. In many web applications, data producers upload their data to servers, And consumers can either directly contact the server or locate the server through a search engine; in many peer-to-peer data sharing applications, directories are used to map data names to their locations. Though these methods have proven success in their intended systems, they are unsuitable for the anytime-anywhere personal sensing. In personal sensing, there is no fixed relationship between data producers and consumers. Data are more likely to be produced unintentionally than purposefully, and the value of the data is discovered postfacto. Consequently, we may end up having much more data than what will be needed later, and uploading these data can place a huge burden on the underlying network.

In addition, privacy can be a serious concern in a server-centric solution as well. This relationship, We.e., having many more producers than consumers, is opposite from what we have observed in other systems, and thus calls for a new data sharing architecture. To address this challenge, we take inspiration from reallife solutions. Suppose if we lost/found an item, a common practice is to post a note around the area where it was lost/ found, and later we refer back to the same location to check for further updates. Similarly, in the anytime-anywhere mobile sensing era, information is commonly tagged with location, thus encouraging location-based queries. To facilitate such queries, we advocate building “directories” around locations of interest by having nearby mobiles carry the data (or the metadata of these data) generated around these locations. We refer to the directory information as the Geocache of the To facilitate such 3queries, we advocate building “directories” around locations of interest by having nearby mobiles carry the data (or the metadata of these data) generated around these locations. We refer to the directory information as the Geocache of the locationl and the location of interest as anchor location. By always having the node close to the anchor location carry the Geocache, we can tie the data around the location where they were generated, thus easily facilitate location-based queries directing them to the corresponding anchor locations using any of the georouting or geocasting techniques. Once the Geocache for an anchor location reaches a certain size, we have the options of compressing the data, or applying the “chaining” technique, which retains only the latest Geocache entries around the anchor location while saving a link to the storage of older entries. Finally, we delete outdated or trivial entries. In this paper, We study protocols that retain Geocache around the anchor location through intervehicle communication. Specifically, WE address two major challenges: 1) returning the Geocache to the anchor location with high probability if the carrier of the Geocache becomes temporarily disconnected; 2) minimizing the communication overhead for retaining the Geocache near an anchor location. WE have presented the trajectory-based boomerang protocol to periodically make available data at certain geographic locations in a highly mobile vehicular network. The boomerang protocol returns the Geocache through nodes traveling toward the anchor location. To increase the

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Special Issue 11, March 2016

probability of successful return, it records a node's trajectory while moving away from the anchor location then select nodes to return the Geocache based on the trajectory (RevTraj).). WE compared this scheme with a shortest distance georouting scheme MaxProgress, and demonstrated that our scheme significantly outperforms its counterpart in realistic traffic simulation, with a return probability improvement of up to 70 percent. . WE also extend the boomerang protocol to satisfy more stringent anchoring requirements, such as returning the Geocache within specified time limits. This is achieved through adapting the initial handoff time based on the return time history.This boomerang protocol addresses the challenges by using a trajectory-based approach. It increases the successful return probability of the Geocache even in temporary disconnected scenarios. While the boomerang protocol is inspired by delay-tolerant geographic routing, it is unique in recording a node's trajectory as the node is moving away from the anchor location and using this trajectory as a guidance to carry back the Geocache. Further, to reduce communication overhead, instead of each node sending the Geocache over the wireless link as soon as it was received, we have the node keep the Geocache until it drives off the original trajectory. Thus, it exploits an important characteristic of vehicular networks, which is: vehicles move on well defined and usually bidirectional paths. WE have showed through analysis and simulations how this characteristic impacts the performance. In connected networks, the increased return probability allows significantly reduced communication overhead by purposefully allowing a node to briefly carry the information away from the anchor location before returning it, instead of constantly keeping the Geocache at the anchor location.

II SYSTEM ANALYSIS

A) EXISTING SYSTEM

The impact of node selfishness on MANETs has been studied in credit-payment scheme. In credit-payment scheme it is shown that when no selfishness prevention mechanism is present, the packet delivery rates become seriously degraded, from a rate of 80 percent when the selfish node ratio is 0, to 30 percent when the selfish node ratio is 50 percent. The number of packet losses is increased by 500 percent when the selfish node ratio increases from 0 to 40 percent. A more detailed study shows that a moderate concentration of node selfishness (starting from a 20 percent level) has a huge impact on the overall performance of MANETs, such as the average hop count, the number of packets dropped, the offered throughput, and the probability of reachability. In VANETs, selfish nodes can seriously degrade the performance of packet transmission. For example, in two-hop relay schemes, if a packet is transmitted to a selfish node, the packet is not re-transmitted, therefore being lost.

Disadvantages of Existing System

- Increase the selfish nodes
- Increase the packet loss
- Reduce the throughput
- Increase overhead

In VANETs, selfish nodes can seriously degrade the performance of packet transmission. For example, in two-hop relay schemes, if a packet is transmitted to a selfish node, the packet is not re-transmitted, therefore being lost.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Special Issue 11, March 2016

B) PROPOSED SYSTEM:

❖ This project introduces Collaborative Contact-based Watchdog (CoCoWa) as a new scheme for detecting selfish nodes that combines local watchdog detections and the dissemination of this information on the network. If one node has previously detected a selfish node it can transmit this information to other nodes when a contact occurs. This way, nodes have second hand information about the selfish nodes in the network.

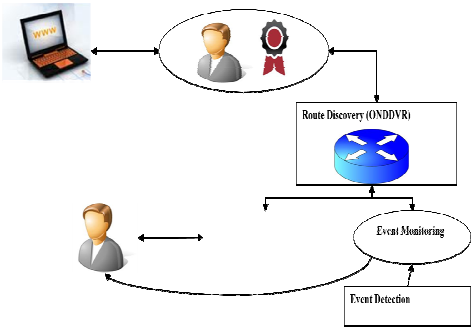
❖ The goal of our approach is to reduce the detection time and to improve the precision by reducing the effect of both false negatives and false positives. In general, the analytical evaluation shows a significant reduction of the detection time of selfish nodes with a reduced overhead when comparing CoCoWa against a traditional watchdog.

❖ The impact of false negatives and false positives is also greatly reduced. Finally, the pernicious effect of malicious nodes can be reduced using the reputation detection scheme. We also evaluate CoCoWa with real mobility scenarios using well known human and vehicular mobility traces.

Advantages of Proposed System

- ✓ Reduce the selfish nodes
- ✓ Increase the throughput
- ✓ Decrease the overhead

III. ARCHITECTURE DESIGN



Geo caching is an outdoor recreational activity in which the participants use a Global Positioning System (GPS) receiver or mobile deviceand other navigational techniques to hide and seek containers, called "geo caches" or "caches", anywhere in the world. A typical cache is a small waterproof container containing a logbook where the geocacher enters the date they found it and signs it with their established code name. Larger containers such as plastic storage containers (Tupperware or similar) or ammunition boxes can also contain items for trading, usually toys or trinkets of little value. Geo caching shares many aspects with benchmarking, trigpointing, orienteering, treasure-hunting, letterboxing, and way marking.

In many itb applications, data producers upload their data to servers, and consumers can either directly contact the server or locate the server through a search engine; in many peer-to-peer data sharing applications, directories are used to map data names to their locations. Though these methods have proven success in their intended systems, they are unsuitable for the anytime-anywhere personal sensing. In personal sensing,

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Special Issue 11, March 2016

there is no fixed relationship betiten data producers and consumers. Data are more likely to be produced unintentionally than purposefully, and the value of the data is discovered postfacto. Consequently, it may end up having much more data than what will be needed later, and uploading these data can place a huge burden on the underlying network.

In addition, privacy can be a serious concern in a server-centric solution as itll. This relationship, i.e., having many more producers than consumers, is opposite from what it have observed in other systems, and thus calls for a new data sharing architecture. To address this challenge, it take inspiration from reallife solutions. Suppose if it lost/found an item, a common practice is to post a note around the area where it was lost/ found, and later it refer back to the same location to check for further updates. Similarly, in the anytime-anywhere mobile sensing era, information is commonly tagged with location, thus encouraging location-based queries.

This paper introduces Collaborative Contact-based Watchdog (CoCoWa) as a new scheme for detecting selfish nodes that combines local watchdog detections and the dissemination of this information on the network. If one node has previously detected a selfish node it can transmit this information to other nodes when a contact occurs. This way, nodes have second hand information about the selfish nodes in the network.

The goal of our approach is to reduce the detection time and to improve the precision by reducing the effect of both false negatives and false positives. In general, the analytical evaluation shows a significant reduction of the detection time of selfish nodes with a reduced overhead when comparing CoCoWa against a traditional watchdog. The impact of false negatives and false positives is also greatly reduced. Finally, the pernicious effect of malicious nodes can be reduced using the reputation detection scheme. It also evaluate CoCoWa with real mobility scenarios using itll known human and vehicular mobility traces.

IV. MODULE DESCRIPTION

ROUTING

The key component is trajectory recording: the aggregated path the pervious carriers have traveled so far. The trajectory grows when a carrier is moving away from the anchor location, and shrinks when it's moving toward the anchor location. Depending on the storage and processing power available on the mobile units, we can use either raw GPS traces or "segmented" trajectory which only consists of the critical points on the path.The handoff procedure used:

Handoff initiation.

Nonfirst time Handoff occurs a divergence is detected from the recorded trajectory. The current carrier broadcasts the Geocache along with the trajectory.

Candidate identification.

Every node within the radio range pops out the latest segments from the trajectory stack. We use a parameter, lookahead distance (LD), to limit how many recent segments we examine. These lookahead segments can be numbered as seg1; seg2; :::segLD, with seg1 being the latest segment. If the node finds itself on one of these lookahead segments, it becomes a candidate node and proceeds to the next step.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Special Issue 11, March 2016

Candidate prioritization.

All the candidates are prioritized according to the following rules:

a) Nodes travelling on higher numbered segments are granted higher priority than those on lower numbered segments;

b) For nodes travelling on the same segment,

we give higher priority to those closer to the anchor location.

ADAPTIVE HANDOFF FOR In-time ANCHORING

Geocache is required to return to the anchor location within a specific time interval. A wide range of mobile applications have such requirements. Nodes are mobile equipment and can move freely from one area to another. A group of users with a large range of mobility can access around in the overall network cause high traffic. In these heterogeneous networks, resources are shared among all users and the amount of available resources is determined by traffic load. The traffic load can seriously affect on quality of services for users thus it requires efficient management in order to improve service quality. If traffic load is concentrated in a cell, this cell becomes the hotspot cell. There is a need to have a proper traffic driven handoff management scheme, so that users will automatically move from congested cell to allow the network to dynamically self-balance.

BOOMERANG

The mobile node that currently carries the Geocache (referred to as the carrier) is moving away from the anchor location. To avoid taking the Geocache away, it hands off the data to other nodes, preferably those traveling toward the anchor location. After receiving the data, the new carrier node will periodically examine whether another handoff is needed. This process repeats until the data returns to the anchor location, and we call this protocol a boomerang protocol because the data eventually return to its origin like a boomerang.

DATA PREPROCESSING AND TRAJECTORY RECORDING

In this, we need to construct trajectories from location (latitude and longitude) recordings reported by the GPS. First, we aggregate consecutive samples with little spatial distance in between (20 m in our experiments), to reduce sample noise. Next, we segmentize the path, retaining only critical turning points by comparing the heading difference between the node's driving direction and the direction of the current segment.

DIVERGENCE DETECTION

When on the return path to the anchor location, a node shrinks the saved trajectory by removing segments it has passed. Meanwhile, it also needs to continuously check if it has diverged from the remaining trajectory. Intuitively, a divergence from the trajectory will result in a noticeable change in the heading direction, as well as a distance increase from the trajectory. However, using one factor alone to determine divergence could be erroneous. Lane shift, the individual's driving behavior and many other factors may all lead to a sudden direction change without actual divergence. Further, the variance in road widths (e.g., 15 to 60 ft for city roads2) makes the selection of a single distance threshold difficult.

In our divergence detection algorithm, we monitor the following conditions when new GPS data are generated:

1) If the distance d between the current location and the trajectory has exceeded the

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Special Issue 11, March 2016

distance threshold d0, and the heading change has exceeded the heading threshold h0,

2) If d has exceeded the maximum road width dmax. Divergence is declared if either condition is met for k consecutive GPS readings.

V. CONCLUSION & FUTURE ENHANCEMENT

This paper proposes CoCoWa as a collaborative contact-based watchdog to reduce the time and improve the effectiveness of detecting selfish nodes, reducing the unsafe effect of fake positives, false negatives and malicious nodes. CoCoWa is based on the distribution of the known positive and negative detections. When a contact occurs among two shared nodes, the distribution element transmits and processes the positive (and negative) detections.

REFERENCEs

1 S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat. Lightweight sybil attack detection in manets. Systems Journal, IEEE, 7(2):236–248, June 2013.

2 S. Bansal and M. Baker. Observation-based cooperation enforcement in ad hoc networks. arXiv:cs.NI/0307012, 2003.

3 S. Buchegger and J.-Y. Le Boudee. Self-policing mobile ad hoc networks by reputation systems. Communications Magazine, IEEE, 43(7):101 – 107, jul. 2005.

4 Buttya´n, Levente, Hubaux, and Jean-Pierre. Enforcing service availability in mobile ad-hoc WANs. In Proceedings of MobiHoc'00, pages 87–96. IEEE Press, 2000.

5 L. Buttya´n and J.-P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Networks and Applications, 8:579–592, 2003.

6 H. Cai and D. Y. Eun. Crossing over the bounded domain: From exponential to power-law intermeeting time in mobile ad hoc networks. Networking, IEEE/ACM Transactions on, 17(5):1578 –1591, oct. 2009.

7 A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott. Impact of human mobility on opportunistic forwarding algorithms. IEEE Transactions on Mobile Computing, 6:606–620, June 2007.

8 J. R. Douceur. The sybil attack. In Revised Papers from the First International Workshop on Peer-to-Peer Systems, IPTPS '01, pages 251– 260, London, UK, UK, 2002. Springer-Verlag

9 S. Eidenbenz, G. Resta, and P. Santi. The COMMIT protocol for truthful and cost-efficient routing in ad hoc networks with selfish nodes. IEEE Transactions on Mobile Computing, 7(1):19–33, Jan. 2008.

10 W. Gao, Q. Li, B. Zhao, and G. Cao. Multicasting in delay tolerant networks: a social network perspective. In Proceedings of ACM MobiHoc '09, pages 299–308. ACM, 2009.