International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 4 Issue 2, February 2017

ISSN: 2394-4404

Performance Evaluation And Detecting Selfish Nodes In DTNS

S. Karthika
Research Scholar,
Cauvery College for Women, Trichy, India

Mrs. P. Rajeswari
MCA.,M.Phil., Associate Professor,
Cauvery College for Women, Trichy, India

Abstract: ***Mobile ad-hoc networks (MANETs) 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 a 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 while detecting selfish nodes, in term of precision and speed. It is especially 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. The 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. The collaborative approach reduces the time and increases the precision when detecting selfish nodes.***

Keyword: ***Wireless networks, MANETs, opportunistic and delay tolerant networks, selfish nodes, performance evaluation.***

I. INTRODUCTION

The past year, empirical studies have provided evidence suggesting that power laws characterize diverse aspects of human mobility patterns, such as inter-contact times, contact, and pause durations. These studies are of high practical importance for (a) informed decisions in protocol design, and (b) realistic mobility models for protocol performance evaluation. Specifically, were perhaps the first to report credible empirical evidence suggesting that the CCDF (complementary cumulative distribution function) of inter-contact time between human-carried mobile devices follows a power law over a wide range of values that span the timescales of a few minutes to half a day.

This empirical finding has motivated to pose the hypothesis that inter-contact time has a CCDF with power law tail. Under this assumption, they derived some interesting results on the feasibility and performance of opportunistic forwarding algorithms. In particular, their hypothesis implies that for any forwarding scheme the mean packet delay is infinite, if the power-law exponent of the inter-contact time is smaller than or equal to 1 (the case suggested to hold in practice by the empirical results so far). These results are in sharp contrast with previously known findings on similar packet forwarding algorithms which were obtained under a hypothesis of exponentially decaying CCDF of inter-contact time. Furthermore, the authors argued that the power-law tail is not supported by common mobility models (e.g. random waypoint), thus suggesting a need for new models.

In this paper, we find that the CCDF of inter-contact time between mobile devices features a dichotomy described as follows. On the one hand, in many cases the CCDF of inter-contact time follows closely a power-law decay up to a characteristic time, which confirms earlier studies. On the other hand, beyond this characteristic time, the find that the decay is exponential. This exponential decay appears to be a new finding, which the validate across a diverse set of mobility traces.

The dichotomy has important implications on the performance of opportunistic forwarding algorithms and implies that recent statements on performance of such algorithms may be over-pessimistic. The further provide analytical results showing that simple mobility models such as simple random walk on a circuit (one-dimensional version of the Manhattan Street Network model dating from the 80's and used recently) and random waypoint on a chain can exhibit the same qualitative properties observed in empirical traces. Whilst our results do not suggest that the considered mobility models are sufficient for realistic simulations, they stress that existing models should not be discarded on the basis of not supporting the empirically observed dichotomy of inter-contact time.

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 opportunistic and delay tolerant networks (DTNs). 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.

Thus, in the real world, nodes could have a selfish behaviour, being unwilling to forward packets for others. Selfishness means that some nodes refuse to forward other nodes' packets to save their own resources. The literature provides two main strategies to deal with selfish behaviour: a) motivation or incentive based approaches, and b) detection and exclusion. The first approach, tries to motivate nodes to actively participate in the forwarding activities. These approaches are usually based on virtual currency and/or game theory models. The detection and exclusion approach is a straight-forward way to cope with selfish nodes and several solutions have been presented. In CoCoWa, which do not attempt to implement any strategy to exclude selfish nodes or to incentivize their participation; instead, the focus on the detection of selfish nodes. The impact of node selfishness on MANETs has been studied in 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.

II. PROBLEM DEFINITION

A simple incentive mechanism for P2P systems is the "tit-for-tat" strategy, where peers receive only as much as they contribute. A free rider that does not upload data chunks to other peers cannot get data chunks from them and suffers from poor streaming quality. Due to its simplicity and fairness, this scheme has been adopted by BitTorrent. Though this strategy can increase the cooperation between peers to a certain level, it is shown in literature that it may perform poorly in today's internet environment due to the asymmetry of the upload and download bandwidths. Unlike the "tit-for-tat" strategy, which enforces compulsory contribution from peers, another category of incentive mechanisms stimulate peers to contribute to the system by indirect reciprocity. In these incentive mechanisms, the contribution of each peer is converted to a score which is then used to determine the reputation or rank of the peer among all the peers in the network. Peers with a high reputation are given a certain priority in utilizing the network resources, such as selecting peers or desirable media data chunks. Therefore, peers with a high reputation have more flexibility in choosing desired data suppliers and thus are more likely to receive high-quality streaming. On the other hand, peers with a low reputation have quite limited options in parent-selection and thus receive low-quality streaming. Through this way, the P2P systems can provide differentiated service to peers with different reputation values. Hence, peers are motivated to contribute more to the P2P system to earn a higher reputation.

A. PROBLEM ANALYSIS

The existing Previous works have demonstrated that watchdogs are appropriate mechanisms to detect misbehaving and selfish nodes. Essentially, watchdog systems overhear wireless traffic and analyze it to decide whether neighbor nodes are behaving in a selfish manner. When the watchdog detects a selfish node it is marked as a positive detection (or a negative detection, if it is detected as a non selfish node). Nevertheless, watchdogs can fail on this detection, generating false positives and false negatives that seriously degrade the behavior of the system. Another source of problems for cooperative approaches is the presence of colluding or malicious nodes. In this case, the effect can even be more harmful, since these nodes try to intentionally disturb the correct behavior of the network.

B. PROBLEM SOLUTION

The proposed 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. Although some of the aforementioned papers introduced some degree of collaboration on their watchdog schemes, the diffusion is very costly since they are based on periodic message dissemination.

III. PROCESS FLOW

A. DEVELOPING PSEUDONYM MANAGER

This module is used to provide cryptography security to the user. The user must first contact the Pseudonym Manager (PM) and demonstrate control over a resource; for IP-address blocking, the user must connect to the PM directly (i.e., not through a known anonymizing network).

B. SERVER REGISTRATION WITH AUDITING

To participate in the Monitoring system, a server with identity id initiates a type-Auth channel to the PM, and registers with the PM according to the Server Registration protocol below.

- ✓ Each server may register at most once in any linkability window.
- ✓ The PM makes sure that the server has not already registered.
- ✓ The PM reads the current time period and linkability Window Blacklisting anonymous users. We provide a means by which servers can blacklist users of an anonymizing network while maintaining their privacy.

C. USER REGISTRATION WITH AUDITING

A user with identity uid must register with the PM once in each linkability window. To do so, the user initiates a type-Basic channel to the PM, followed by the User Registration protocol described below.

- ✓ The PM checks if the user is allowed to register. In our current implementation, the PM infers the registering user’s IP address from the communication channel, and makes sure that the IP address does not belong to a known exit node. If this is not the case, the PM terminates with failure.
- ✓ Otherwise, the PM reads the current linkability window

D. AUDITING AND FILING FOR COMPLAINTS

If at some later time, the server desires to blacklist the user behind a Monitoring connection, during the establishment of which the server collected ticket from the user, the server files a complaint for the future reference.

E. BLACKLISTING A USER

If a user misbehaves, the server may link any future connection from this user within the current linkability window. Even though misbehaving users can be blocked from making connections in the future, the users’ past connections remain unlinkable, thus providing backward unlinkability and subjective blacklisting.

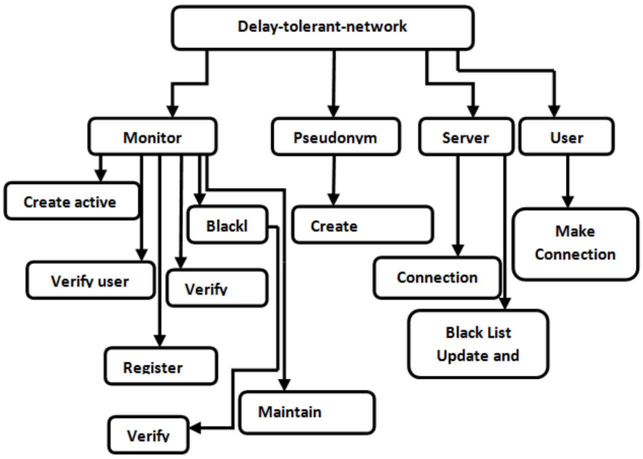
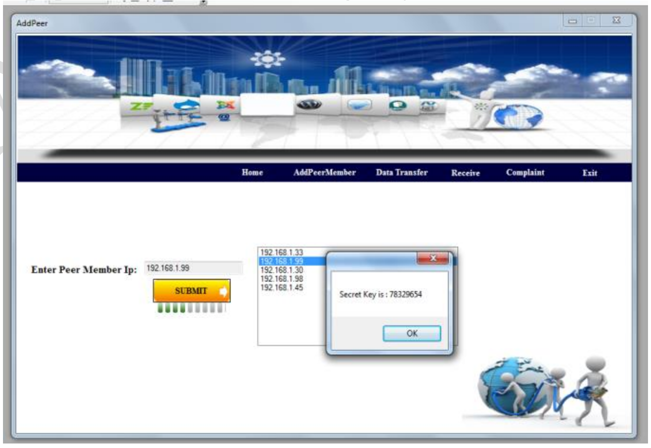


Figure 1: Process Flow

IV. EXPERIMENTAL RESULTS

A. IMPLEMENTATION

More recently, papers have focused on DTNs. In the author introduces a model for DTN data relaying schemes under the impact of node selfishness. A similar approach is presented in that shows the effect of socially selfish behaviour. Social selfishness is an extension of classical selfishness (also called individual selfishness). A social selfish node can cooperate with other nodes of the same group, and it does not cooperate with other nodes outside the group. The impact of social selfishness on routing in DTN has been studied in Our approach presents similarities with the ones presented. Nevertheless, these approaches do not evaluate the effect of false positives, false negatives and malicious nodes. For example, the approach in only transmits positive detections. The problem, as shown in the evaluation sections, is that if a false positive is generated it can spread this wrong information very quickly on the network, isolating nodes that are not selfish. Therefore, an approach that includes the diffusion of negative detections as well becomes necessary. Another implementation issue is the high imposed overhead due to the flooding process in order to achieve a fast diffusion of the information. Since our approach is based on contacts, it has been proven that the overhead is greatly reduced.

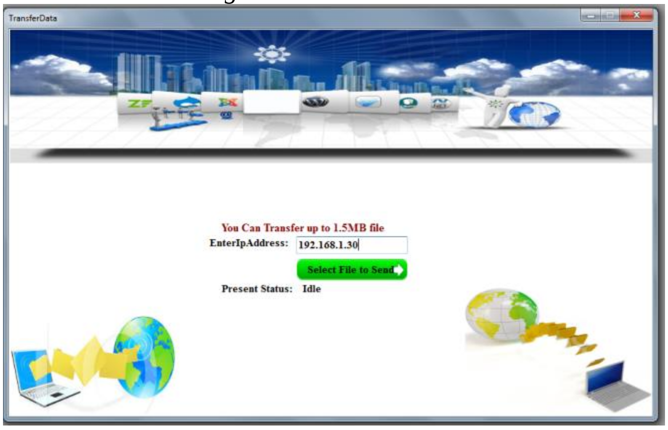


Enter Peer Member Ip: 192.168.1.99

192.168.1.33
192.168.1.99
192.168.1.30
192.168.1.98
192.168.1.45

Secret Key is : 78329654

Figure 2: Node Creation

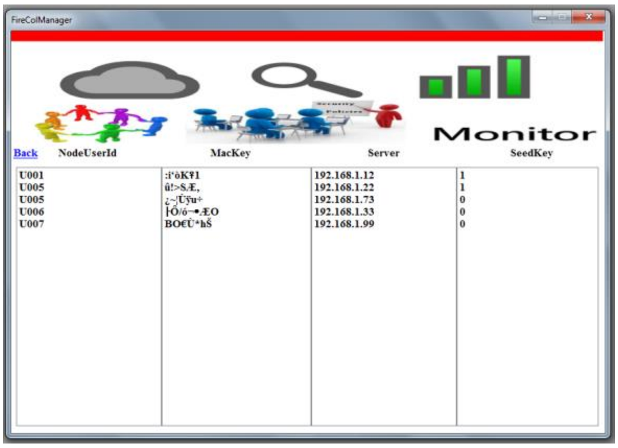


You Can Transfer up to 1.5MB file

EnterIpAddress: 192.168.1.30

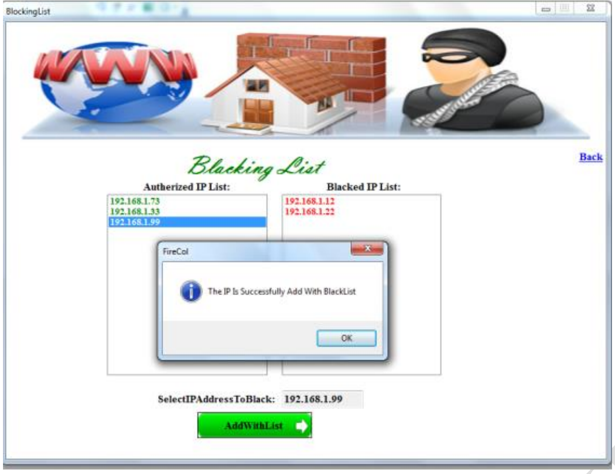
Present Status: Idle

Figure 3: Server Waiting to Receive Data



Back NodeUserId	MacKey	Server	SeedKey
U001	:i'òK₮1	192.168.1.12	1
U005	û!>S.Æ,	192.168.1.22	1
U005	¿~¦Ûÿu+	192.168.1.73	0
U006	├Ô/ó¬•ÆO	192.168.1.33	0
U007	BO€Ù*hŠ	192.168.1.99	0

Figure 4: Monitor Node



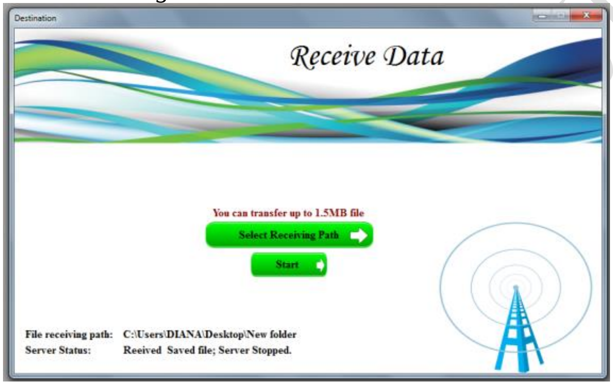
Autherized IP List:
192.168.1.73
192.168.1.33
192.168.1.99

Blacked IP List:
192.168.1.12
192.168.1.22

FireCol
The IP Is Successfully Add With BlackList
OK

SelectIPAddressToBlack: 192.168.1.99

Figure 4: Blacklist Maintenance



You can transfer up to 1.5MB file

File receiving path: C:\Users\DIANA\Desktop\New folder
Server Status: Reeived Saved file; Server Stopped.

Figure 6: Receive Packet Successfully

V. RESULT AND DISCUSSION

The performance comparison is based on two metrics: detection rate and false positive rate. The categories of the "neighbor's nature" and "cut-off decision" combinations are calculated. For each combination, we sum up all the decisions made by good nodes (evil nodes' cut-off decisions are irrelevant) and obtain four counts: TP (true positives), FN (false negatives), TN (true negatives), and FP (false positives). The detection rate DR is defined as

$$DR = \frac{TP}{TP+FN} \times 100\%,$$

and the false positive rate FPR is defined as

$$FPR = \frac{FP}{FP+TN} \times 100\%.$$

A high detection rate and a low false positive rate are desirable. When a balance must be stricken between the two, one might be emphasized over the other, depending on the context. We compare the two alternative approaches; distribution and maximize, to the look-ahead strategy. The look-ahead parameter reflects a node's intrinsic (infection) risk inclination. In both Haggle and MIT reality, the robust cutoff strategy with a larger corresponds to a higher detection rate (in the early stage for Haggle and throughout for MIT reality) and a significantly lower false positive rate (for both data sets). In Haggle, the eventual detection rates for all three look-ahead parameters are close to 100 percent. The difference in the eventual detection rate between Haggle and MIT reality is attributed to the different contact patterns in these data sets: The contact pattern in Haggle is more homogeneous than that in MIT reality, in the sense that the variation of the interval between encounters is significantly higher and a few nodes contribute most of the assessments in MIT reality. Thus, the detection rate is more sensitive to the change of in MIT reality than in Haggle. In both data sets, the detection-rate and false-positive rate are comparable for the distribution and maximize approach, with the distribution approach having a slightly higher detection rate and false-positive rate.

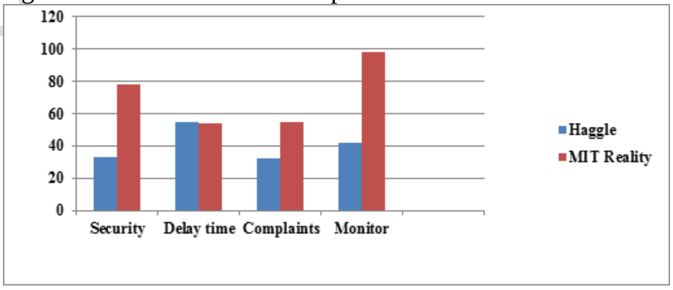


Figure 7: Performance comparison

In traditional, non-DTN, networks extend the Naive Bayesian model, which has been applied in filtering email spams, detecting botnets , and designing IDSs, and address DTN-specific, malware-related, problems. Presented a distributed IDS architecture of local/global detector that resembles the neighborhood-watch model, with the assumption of attested/honest evidence, i.e., without liars.

- ✓ Given enough assessments, honest nodes are likely to obtain a close estimation of a node's suspiciousness (suppose they have not cut the node off yet), even if they only use their own assessments.
- ✓ The liars have to share a significant amount of false evidence to sway the public's opinion on a node's suspiciousness.
- ✓ The most susceptible victims of liars are the nodes that have little evidence.

VI. CONCLUSION

This paper proposes CoCoWa as a collaborative contact-based watchdog to reduce the time and improve the effectiveness of detecting selfish nodes, reducing the harmful effect of false positives, false negatives and malicious nodes. CoCoWa is based on the diffusion of the known positive and negative detections. When a contact occurs between two collaborative nodes, the diffusion module transmits and processes the positive (and negative) detections. Analytical and experimental results show that CoCoWa can reduce the overall detection time with respect to the original detection time when no collaboration scheme is used, with a reduced overhead (message cost). This reduction is very significant, ranging from 20 percent for very low degree of collaboration to 99 percent for higher degrees of collaboration. Regarding the overall precision we show how by selecting a factor for the diffusion of negative detections the harmful impact of both false negatives and false positives is diminished. Finally, using CoCoWa we can reduce the effect of malicious or collusive nodes. If malicious nodes spread false negatives or false positives in the network CoCoWa is able to reduce the effect of these malicious nodes quickly and effectively.

REFERENCES

[1] “Performance modeling of epidemic routing” Xiaolan Zhang a,*, Giovanni Neglia b, Jim Kurose a, Don Towsley a, a Department of Computer Science, University of Massachusetts, Amherst, MA 01003, United States, b Universita` degli Studi di Palermo, Italy, Received 1 October 2006; accepted 20 November 2006, Available online 19 December 2006

[2] ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-hop Wireless Networks Mohamed Elsalih Mahmoud, and Xuemin (Sherman) Shen, IEEE Fellow.

[3] The Sybil Attack John R. Douceur *Microsoft Research,johndo@microsoft.com*

[4] Observation-based Cooperation Enforcement in Ad hoc Networks, Sorav Bansal Mary Baker Stanford University Stanford, CA 94305, USA, sbansal@stanford.edu, mgbaker@cs.stanford.edu

[5] Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks Levente Butty´an and Jean-Pierre Hubaux, Laboratory for Computer Communications and Applications, Swiss Federal Institute of Technology – Lausanne, EPFL-IC-LCA, CH-1015 Lausanne, Switzerland, March 19, 2002.

[6] Power Law and Exponential Decay of Inter Contact Times between Mobile Devices Thomas Karagiannis, Microsoft Research, Cambridge, UK, thomkar@microsoft.com

[7] Characterising aggregate inter-contact times in heterogeneous opportunistic networks, Andrea Passarella and Marco Conti, IIT-CNR, Via G. Moruzzi 1, 56124 Pisa, Italy, {a.passarella, m.conti}@iit.cnr.it.

[8] “Multicasting in delay tolerant networks: A social network perspective,” in Proc. W. Gao, Q. Li, B. Zhao, and G. Cao, 10th ACM Int.Symp. Mobile Ad Hoc Netw. Comput., 2009, pp. 299–308.