RESEARCH ARTICLE OPEN ACCESS

Efficient Detection Of Selfish Node In Manet Using A Colloborative Watchdog

S.Lavanyak.Pavithra[1], P.Prema[2]
[1]*Dept .of Computer Science and Engineering*
[2]*Assistant Professor Dhanalakshmi College of Engineering*

ABSTRACT
Mobile ad-hoc networks(MANET) are collected many number of nodes.In a mobile ad-hoc network(MANET) undertakes that all the mobile nodes unitewillingly in order to work accurately.This is a cost –intensive action for the collaboration and particular nodes can decline to cooperate then it will prominent to a selfish node behaviour.Thus, it will utterly affect the global network performance.The watchdogs are a well-known device used for identifying a selfish node.Theprocedure performed by watchdogs can fail,generating false positives and false negatives this may convince to wrong operation.Whenidentifying selfish node trusting on local watchdogs only can prime to poor performance,in terms of precision and speed.Thus we propose collaborative contact based watchdog(COCOWA) as a collaborative method based on the dispersion of selfish nodes responsiveness when a contact occurs,so the evidence will quickly circulated about selfish nodes. As shown in the paper,whenidentifying a selfish nodes this collaborative approach decreases the time and rises the precision.

I. INTRODUCTION

Mobile ad-hoc networks (MANETs) adopt that mobile nodes intended unite in order to work properly. This cooperation is a cost-exhaustive activity and some nodes can refuse to cooperate, leading to a selfish node behaviour. Thus, the overall network performance could be totally affected. The use of watchdogs is a well-known machine to detect selfish nodes. Conversely, the detection process completed by watchdogs can fail, engendering false positives and false negatives that can convince to wrong tasks. Moreover, trusting on local watchdogs unaided can lead to poor presentation when detecting selfish nodes, in term of correctness and rapidity. This is specially important on networks with sporadic contacts, such as delay tolerant networks (DTNs), where occasionally watchdogs lack of enough time or material to detect the selfish nodes. Thus, we suggest collaborative contact based watchdog (CoCoWa) as a collaborative method based on the diffusion of local selfish nodes attention when a contact occurs, so that information about selfish nodes is quickly publicized. As shown in the paper, this collaborative approach diminishes the time and increases the accuracy when detecting selfish nodes.

II. EXISTING SYSTEM

In these styles do not estimate the conclusion of false positives, false negatives and malicious nodes. For example, the methodology only transfers positive detections. The difficult, as shown in the evaluation sections, is that if a false positive is produced it can supper this wrong evidence very rapidly on the network, separating nodes that are not selfish. Therefore, an approach that includes the distribution of negative detections as well converts necessary. Another problem is the power of colluding or malicious nodes. Although a reputation system can be convenient to moderate the result of malicious nodes, it clearly depends on how are united local and global ratings, as shown in this paper. Another execution issue is the high levied overhead due to the submerging process in command to complete a fast circulation of the evidence.

III. PROPOSED SYSTEM

This paper proposes CoCoWa as a collaborative contact-based watchdog to decrease the period and expand the usefulness of perceiving selfish nodes, falling the dangerous effect of false positives, false negatives and malicious nodes. CoCoWa technique is used to perceive Sybil attack, black whole attack and redirect attack. Nodes is confronted by Sybil attack,(i)it will forward the data but it won't acknowledge to the source,(II)it won't forward the data but it will acknowledge to the source. Black whole attack it will interprets the data. Redirect attack is to forward the data to source. CoCoWa can decrease the overall exposure time with reverence to the inventivefinding time when collaboration scheme is not allotted, with a condensed overhead (message cost).

IV. OVERALL DESCRIPTION

4.1 Product Perspective

In these methods do not value the effect of false positives, false negatives and malicious nodes. For example, the style only transmits positive detections. The problem, as shown in the evaluation sections, is that if a false optimistic is produced it can range this wrong material very speedily on the network, isolating nodes that are not selfish. Therefore, an approach that includes the diffusion of negative detections as well becomes necessary. Another problem is the impact of colluding or malicious nodes. Although a reputation system, can be beneficial to lessen the outcome of malicious nodes, it obviously depends on how are mutual local and global ratings. Another operation issue is the high obligatory overhead due to the flooding process in order to achieve a fast diffusion of the information

4.2 Product Features

This paper proposes CoCoWa as a collaborative contact-based watchdog to condense the stretch and progress the success of perceiving selfish nodes, tumbling the harmful outcome of false positives, false negatives and malicious nodes. CoCoWa is created on the diffusion of the known positive and negative detections. When a commerce occurs between two collaborative nodes, the circulation module conducts and progressions the positive (and negative) recognitions. Analytical and investigationaloutcomes show that CoCoWa can diminish the overall recognition time with reverence to the original recognition time when no collaboration structureisused, with a condensed overhead (message cost).

V. EXPERIMENTAL WORK

5.1 Network Formation

Nodes can be fashioned by generousspace and series. Neighbour nodes resolveperceivefounded on exposure and it will modificationvigorously based on movement. Specialist will produce the public key and private key using RSA algorithm. For the straightforwardness of demonstration, we take a three-step data forwarding process as anspecimen. Suppose that node A has packets, which will be transported to node C. Now, if node A encountersadditional node B that capacity help to onward the packs to C, A will repeat and advancing the packages to B. Subsequently, B willheadlong the packets to C when C arrives at the program range of B.

5.2 Route Discovery

The First Contact Routing Protocol can be used to determine the route. In the network the nodule have some reporting and mobility .The neighbor nodes will energetically change in each node founded on its mobility. The route location is based on the source and destination,adjacent node can be choosed to forwarder.

5.3 Data Forwarding

A regularoperator will decentlymonitor the first routing protocol by forwarding the messages as long as there are enough associates. Data can be encoded using Rs.Thedemandedcommunication has been accelerated to the next hop, the selected next hop nodes are necessary nodes rendering to a specific MANET routing protocol, and the quantity of forwarding copies satisfy the requirement positive by a multi-copy forwarding routing protocol.

5.4CollaborativeContact-Based Watchdog (COCOWA)

The compromise between the security and detection cost, Presents a COCOWA, which could launch the collaborative contact based watchdog for the target node and magistrate it by gathering the encouraging history indication from its upstream and downstream nodes. Then COCOWA might punish or recompense the node based on its performances. To further recover the presentation of the proposed colloborative inspection system, we introduce a reputation system, in which the reviewchance could vary along with the target node's reputation. Under the reputation system, a node with a good reputation will be check with a lower probability while a bad reputation node could be checkered with a higher probability. We using the Inspection Game and use game theoretical analysis to demonstrate that COCOWA could ensure the security of MANET routing at a reduced cost via choosing an appropriate investigation possibility.

VI. ALGORITHMS

1. First Contact Routing Protocol
2. Collaborative Contact based watchdog
3. RSA Algorithm

VII. TYPES OF ATTACKS

- **SybilAttack**

The Sybil attack is an attacker subverts the reputation system of peer-to-peer network by creating large number of pseudonymous identities,using them to gain disproportionately large influencesource.

- **Black hole attack**

Black holes refer to that the data sent to destination is dropped without informing it to the source.

❖ **RedirectAttack**

The redirect attack is an attacker that forward the data to each and every nodes when it reaches the attacker node,the attacker node will forward the data to source.

Design& Implementation Constraints

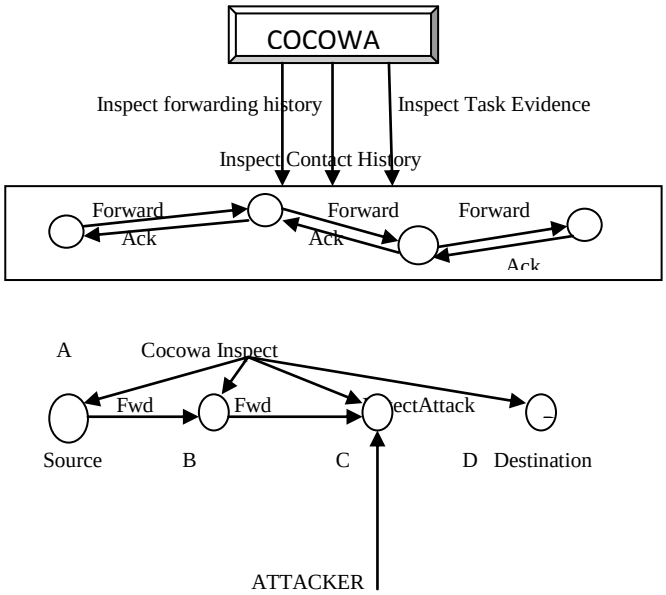
❖ **Constraints in Design**

- Determination of the Involved Classes
- Determination of the Compound Objects
- Determination of the Involved Actions
- Determination of the Require Clauses
- Global actions and RestraintRecognition

❖ **Constraints in Application**

A gradedarranging of relatives may outcome in additionalmodules and extra complicated structure to implement. Therefore it is advisable to transform the hierarchical relation structure toward a simpler structure such as a traditional flat one. It is slightly straightforward to transmute the established hierarchical prototypical into a bipartite, flat model, containing of classes on the one hand and flat associations on the other. Flat associations are chosen at the design level fordetails of simplicity and implementation simplicity. There is no individuality or functionality associated with a flat relation. A flat relation resembles with the relation ideaentity-relationship demonstrating many object oriented methods.

VIII. ARCHITECTURE DIAGRAM



IX. ENHANCEMENTS

9.1 Blackhole Attack

Black holes refer to that the data sent to destination is dropped without informing it to the source.

9.2 Redirect Attack

The redirect attack is an attacker that forward the data to each and every nodes when it reaches the attacker node,the attacker node will forward the data to source.

X. CONCLUSION

Thus we project, to diminishbroadcast overhead suffered by misconductdiscovery and perceive the malicious nodes successfully for secure MANET routing.

REFERENCES

[1]. S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight sybil attack detection in manets," IEEE Syst. J. vol. 7, no. 2, pp. 236–248, Jun. 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," IEEE Commun. Mag., vol. 43, no. 7, pp. 101–107, Jul. 2005.

[4]. L. Butty_an and J.-P.Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in Proc. 1st Annu. Workshop Mobile Ad Hoc Netw.Comput., 2000, pp. 87–96.

[5]. L. Butty_an and J.-P.Hubaux, "Stimulating cooperation in selforganizing mobile ad hoc networks," Mobile Netw.Appl., vol. 8, pp. 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," IEEE/ACM Trans. Netw., vol. 17, no. 5, pp. 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 Trans. Mobile Comput., vol. 6, no. 6, pp. 606–620, Jun. 2007.

[8]. J. R. Douceur, "The sybil attack," in Proc. Revised Papers 1st Int. Workshop Peer-to-Peer Syst., 2002, pp. 251–260.

[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 Trans. Mobile Comput., vol. 7, no. 1, pp. 19–33, Jan. 2008.

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