ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

A Combinatorial Approach to THWART and Mitigate Selfish Attack in MANET

G. Sudhakar[1], Priyanga . M[2]

Assistant Professor and HOD, Department of Computer Science and Engineering, Ranganathan Engineering College, Coimbatore, Tamil Nadu, India[1]

PG Scholar, Department of Computer Science and Engineering, Angel College of Engineering, Ranganathan Engineering College, Coimbatore, Tamil Nadu, India [2]

ABSTRACT: Wireless network utilize the node mobility and opportunistic contact among nodes for data communication, because the network structure infrastructure less. Due to this nature, many types of security threads affect Ad-hoc network process and performance. In this paper, we focused on the selfish attack detection and avoidance with analyzing its impact over ad-hoc network. In the infrastructure free network, the selfish behavior of nodes affects the overall performance of the packet transmission. Usually, the selfish attack can be identified rather than protecting them. The detection of selfish behavior is a challenging one. In this paper, we papered various techniques and methods used to prevent and detect selfish nodes over MANET. This study proposes an improved watchdog technique named as Reputed Information eXchange (RIX) scheme as a collaborative approach based on the diffusion of local selfish nodes awareness when a node is compromised by external attackers. The RIX approach reduces the packet transmission time and increases the precision by detecting the compromised nodes attacked by selfish nodes. The privacy and Security analysis demonstrates that RIX can well protect user selfishness against both inside and outside attackers.

KEYWORDS: MANET, Selfish attacks, watchdog, anonymization, acknowledgements, Evidences.

I. INTRODUCTION

Ad-Hoc networks have free infrastructure where the nodes are free to join and left the network at any time. The nodes are connected with each other via a wireless link in Ad-Hoc network. In this free infrastructure, a node can act as a server as well as client to transmit the data in the network. Therefore this kind of network is also known as infrastructure less networks [1]. These networks have no centralized server or authority. Routing and channel selection are also on demand. Whenever a node in the network is inactive or moves from the network, that causes the link failure. The source node will establish a new channel. Ad-Hoc network can be categorized in to two types named as Mobile Ad-Hoc network (MANET) and Vehicular Ad-hoc networks. In MANET, cooperative structure has been followed, this types of networking provides cost effective services. The cooperation on these networks is always based on contacts. Every mobile node can communicate with each other directly if a contact occurs. Every node performs the same and supports this cooperation, due to the intention of reducing communication cost. Due to this flexible nature, there are several security issues [2] threatens ad-hoc networks. Ad-Hoc networks have the capabilities to handle those issues in different ways.

II. LITERATURE REVIEW

Mobile ad-hoc networks rely on cooperation of all participating nodes; as a result all nodes have a good reputed communication link between all nodes. But some nodes are vulnerable to selfish behavior, and these types of nodes will not provide proper resource allocation. The outlines important attacks and summarizes popular approaches to design secure MANET protocols in order to detect selfish and malicious nodes and to enforce cooperation [3]. The routing misbehavior in MANETs is impact and specifically, the routing protocols for MANETs are designed based on the belief that all participating nodes are fully cooperative and non selfishness. But due to several reasons the node

DOI: 10.15680/IJIRCCE.2016. 0405188

misbehaviors may exist in the network [4]. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. The author from the same paper had a discussion on different schemes are to mitigate and detect routing misbehavior.

Martin Schütte defined the nature of Selfish nodes and its behavior. This could help to find the normal and selfish node in the network [5]. The author gave the definition of selfish Nodes as. The selfish node that does not forward other nodes packets and this will maximize their benefit at other node expenses. They are assumed to always behave rationally. In this paper, the author confesses several definitions of selfish node behavior. The impact of node selfishness on MANETs has been studied in [6] it is shown that the performance of the network is degraded if there is not mechanism for selfishness prevention. As like the above paper, paper shows similar result, where the number of packet drop ratio is increases up to 40%. This study proves the impact of selfishness in network performance [7].

Many different techniques for detection of selfish nodes have been discussed which effect the performance degradation in MANETs [8] The credit-based scheme is to provide incentives in terms of electronic payments/ beans for nodes to faithfully perform networking functions. The watchdog detection mechanism has a very low overhead. Even the watchdog mechanism consumes less overhead, regrettably, that suffers from several problems such as limited transmission power, ambiguous collisions and receiver collisions. A new low cost approach for monitoring node misbehavior in MANET is introduced and the name of the technique is SMDP. It reduces the communication overhead by using only one hop communication instead of flooding, and sending control packets only at the end of sessions. This is not performing for every packet in the transmission.

A. Selfishness Detection techniques

Authors in literature have demonstrated that watchdogs are appropriate mechanisms to detect misbehaving and selfish nodes in ad-hoc networks [9]. Broadly, watchdog systems are considered more efficient technique to detect the selfishness. This eavesdrops on wireless traffic and analyses it to decide, whether neighbor nodes are malicious or legitimate. If the watchdog detects the selfish activities, then it is highlighted as positive detection else that is marked as non-selfish node. The main demerits of this kind of detection technique are it increases false alarms.

The authors presented a method using a virtual currency called nuglet [10] [11]. Later author Zhong et al. proposed SPRITE technique, which is a credit based system to provide incentive to the participation of selfish nodes in MANET [12]. This type of methods created several issues. The issues are common in the MANET, because storing individual data on the server is very problematical. It can be improved by applying some special tamper proof components, Afterward some authors introduced selfish node detection using cooperative models. In this approach, every node actively participates in the group activities such as forwarding the data to the receiver. Most of the routing algorithms designed for MANET such as DSR [13] and AODV [14] are based on the assumption that every node forwards every packet, however some of the nodes may act as the selfish nodes at the time of requisition. These nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes do not consume any energy such as CPU power, battery and also bandwidth for retransmitting the data of other nodes and they reserve them only for themselves.

In existing paper, authors discuss two techniques namely Reputation technique and Credit technique [15] used to detect selfish nodes in MANET. Various algorithms have been designed in recent years to resolve the issue of self-seeking nodes (selfish nodes). Every algorithm takes a different approach to the problem; however the majority of these algorithms can be broken into three general classes. According to the reputation based algorithm, each node is responsible for either keeping track of other nodes in the network, or obtaining the reputation from a centralized node on the network. The reputation score will be increased if a node successfully participates in the transmission of data by forwarding data packets. If the nodes reputation drops below a threshold set by the network, the node is either punished or ignored. A credit based algorithm is similar to a reputation based algorithm. The difference is this algorithm is that each node begins with a set of credits. A node sends a packet to its neighbor node for forwarding. After successfully forwarding the packet, the sending node credits the neighbor as a reward. If nodes do not forward the packet, they will run out of credits resulting in not having the ability to send their own packets.

In a game theory algorithm [17], each node uses previous history to determine the best path to send the packet. The amount of processing power utilized is dependent upon the 3 node. The more power used, the best path can be chosen, but more power is consumed. As a result of the limited amount of power each node has, the node must choose between using a large amount of its power to find the best path, or use a small amount of its power and take chances with an alternate path. In previous works it has been shown how some degree of cooperation can improve the finding of selfish or misbehaving nodes. The CONFIDENT protocol was proposed in [18], which combines a watchdog, reputation systems, Bayesian filters and information obtained from a node and its neighbors' to securely detect misbehaving nodes. The system's response is to isolate those nodes from the network, punishing then indefinitely. A distributed intrusion finding system (IDS) is introduced in [19]. In this approach if a node locally detects an intrusion with strong evidence, it can initiate a response. But, if a node detects an anomaly with weak evidence, it can initiate a cooperative global intrusion finding procedure. A similar approach is the mobile intrusion finding system described in [19]. In this case, local sensor ratings are periodically flooded throughout the network in order to obtain a global rating for each misbehaving node.

In watchdog, a node sends a packet to its neighbor and then observes the neighbor, whether the packet is transferred along the route properly or not. So the malfunctioning and selfish node is immediately identified, but this technique has several drawbacks such as every node should prune the collision information at the time of implementation, to reduce the negative detection.

III. PROBLEM DEFINITION

In the infrastructure free environment, a mobile node may omit the resource request from the neighbor node on certain transaction is stated as selfish behavior. A node would like to enjoy the benefits provided by the resources of other nodes, but it may not make its own resource available to help others. Such selfish behavior can potentially lead to a wide range of problems in adhoc networks. Existing research on selfish behaviors in a MANET mostly focus on network issues. In some cases, nodes can perform this selfish behavior by revealing fake information about their resources. In certain circumstances the nodes might behave normally during the election but then deviate from normal behavior by not offering the IDS service to their voted nodes. The issue in which this thesis addresses is the existence of selfish nodes, specifically those that continuously drop packets, in Mobile Ad Hoc Networks. Selfishness can have disastrous effects within the MANET. Often times, the existence of selfishness don't have such effects as described above. In open systems, usually selfishness only results in loss of data during transmission. If the network is designed correctly, the data can be retransmitted until a successful transmission. Although the data is eventually transmitted successfully, this results in an increase in bandwidth utilization and extra power usage by each of the nodes within the path of the transmission.

IV. PROPOSED SYSTEM

The proposed technique used to combat node misbehavior in network using reputation-based. Using this approach, the network nodes collectively detect and declare the misbehavior and suspicious node and informs to others. Such a declaration is then broadcasted right through the network, so that the misbehaving node will be eliminated or punished from the rest of the network if the score is low. And the selfish nodes will be punished and good nodes will be prioritized along with credit point. The existing watchdog technique failed to detect misbehavior and creates false alarms in the presence of selfish nodes. The system overcomes the above drawback of existing watchdog by implementing a new method, which is the combination of Reputation based schemes. Based on the reputation score and positive score, selfish node will be identified.

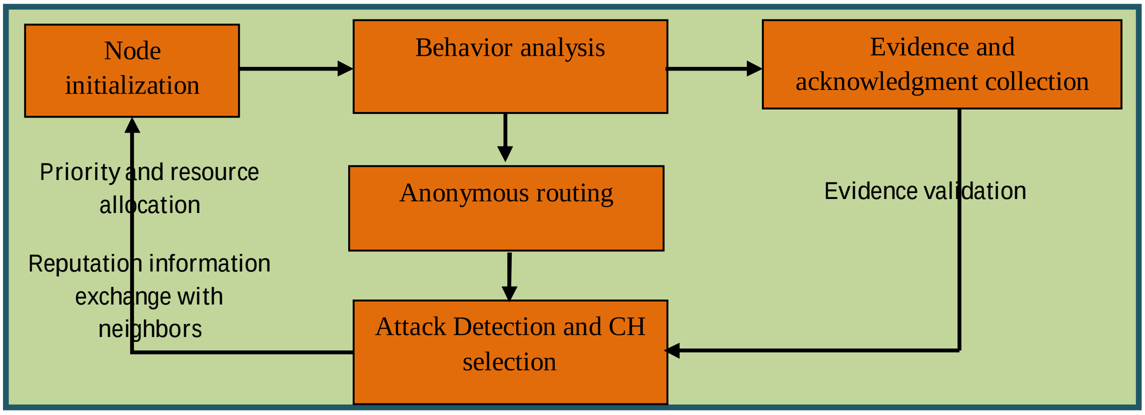
Node initialization
Behavior analysis
Evidence and acknowledgment collection
Priority and resource allocation
Anonymous routing
Evidence validation
Reputation information exchange with neighbors
Attack Detection and CH selection

Fig: 1.0 the overview of the proposed method

DOI: 10.15680/IJIRCCE.2016. 0405188

The above fig1.0 represents the overall process of the proposed framework. This shows all over steps involved from node initialization and information exchange process.

The configuration Phase has two steps such as the initial setup and the user registration. During the initial setup phase, the RIX generates a group an anonymous key and sends announcement with group public key during gateway advertisement. In addition, RIX also publishes the method of generating the tag bases that will be used to send caution, cooperation and event reporting.

Anonymous Key generation and authentication: The Anonymous Key generation performed in this Phase. This Phase initially applies the effective signature creation algorithm can be used for Anonymous Key generation. Additionally the key verification and authentication is required to ensure that services are offered to legitimate entities.

Decision making Phase: This section describes the process of estimating the trust, judging the reputation and how the mobile nodes are categorized as trusted/selfish and genuine/ malicious.

Trust assessment Phase: This phase evaluates the collected acknowledgements and data's with the predefined threshold value and finds the deviation. Based on the information collected and compared by the user, it calculates the direct trust value and stores it into the local table RT (reputation table). The direct trust value is calculated mainly based on the behavior of packet transmission, delay and negative acknowledgements. The indirect trust value is determined based on the information collected from other users in the network and maintained by the common RT.

Reputation Phase: Any user suspects the malicious activity such as holding the packets for a long time or giving false report in the network is performed by any user, it can send a caution at once to that user. Upon receiving a warning, the legitimate user has to send a maximum of one cooperation message using the tag base published in the setup procedure. If the user does not send cooperation or sends multiple cautions is marked as a malicious user.

Identification Phase: In this Phase, the trust value obtained from the trust estimation Phase is compared with the threshold. If the trust value is less than the threshold, then the user can be marked as outlier otherwise trusted. In the same way, based on the reputation obtained from the reputation Phase, the user can be marked as malicious or genuine.

Trust Center (monitor) Phase: In this Phase Trust Center will receive the reports from each node's every performance. This report is verified for the node's activity example best performing and worst performing. The best nodes will get the Ack as resource allocation and priority to be access data first. The penalty will be evicted from the network.

CH selection: In this Phase particular regions leader will be elected based on the previous performance report. The leader should not be act as partial and selfish, if so then the node cannot be able to become a leader in that particular region. This leader will be elected based on the acknowledgment and score provided by the RIX reelection will be performed if the CH node malicious. In this Phase develop a trust system based on processing the different acknowledgements and reports to maintain a trust value for each node. The more trust system can be electing as a leader for that particular cluster. The role of the cluster head is to forward the data of each node in the cluster to sink. So the leader node must need a high bandwidth and other network resources to send.

V. SIMULATION RESULTS

The proposed RIX has successfully verified with 30 nodes. The system has generated three types of acknowledgments and transaction reports. Based on the demonstration, we have generated the results and comparison graph in this section.

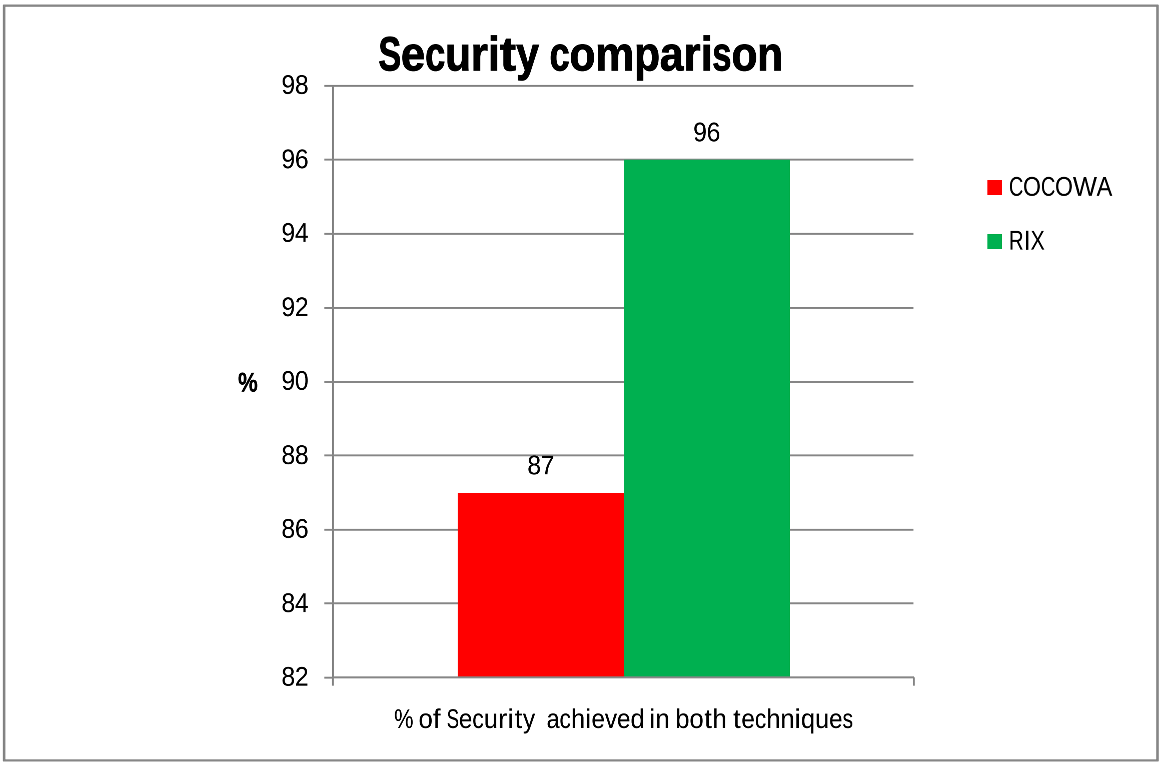

Fig 2.0 comparison chart

The above fig 2.0 shows the security achievements with various feature is compared with the existing system. While comparing with the existing system, the proposed RIX yielded high security feature than the existing COCOWA.

VI. CONCLUSION

The proposed RIX addresses the privacy and selfishness attack issues in MANET. The architecture adapts the modules such as RIX, trust estimation, reputation exchange in order to monitor and determine the mobile nodes trust score and reputation. Based on these feature, the observer will fix the node state and reports to the other users in the network if it is a selfishness node. It also provides anonymous data transformation in order to prevent data from selfishness nodes.

This paper proposes RIX a contact-based watchdog to reduce the time and improve the effectiveness of detecting selfish nodes and reducing the harmful effect of false positives, false negatives and malicious nodes. RIX is based on the diffusion of the known positive and negative acknowledgements. When a contact occurs between two collaborative nodes then the diffusion module transmits and processes the positive (and negative) detections. Analytical and experimental results show that RIX can reduce the overall detection time with respect to the original detection time when no collaboration scheme is involved and this also proved that the message and communication overhead is reduced.

REFERENCES

1. J.-P. Hubaux, T. Gross, J.-Y. L. Boudec, and M. Vetterli, “Toward selforganized mobile ad hoc networks – the terminodes project,” IEEE Communications Magazine, vol. 39, no. 1, pp. 118–124, 2000
2. Li, Wenjia, and Anupam Joshi. "Security issues in mobile ad hoc networks-a survey." Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County (2008): 1-23.
3. Kargl, Frank, et al. "Advanced detection of selfish or malicious nodes in ad hoc networks." Security in Ad-hoc and Sensor Networks. Springer Berlin Heidelberg, 2004. 152-165.
4. Dorri, Ali, Seyed Reza Kamel, and Esmaeil Kheirkhah. "Security challenges in mobile ad hoc networks: a survey." arXiv preprint arXiv:1503.03233(2015).
5. Schütte, Martin. "Detecting selfish and malicious nodes in MANETs."seminar: sicherheit in selbstorganisierenden netzen, hpi/universität potsdam, sommersemester. 2006.
6. Hernandez-Orallo, Enrique, et al. "Improving selfish node detection in MANETs using a collaborative watchdog." Communications Letters, IEEE16.5 (2012): 642-645.
7. Michiardi, Pietro, and Refik Molva. "Simulation-based analysis of security exposures in mobile ad hoc networks." European Wireless Conference. 2002.
8. Koshti, Dipali, and Supriya Kamoji. "Comparative study of techniques used for detection of selfish nodes in mobile ad hoc networks." International Journal of Soft Computing and Engineering (IJSCE) ISSN (2011): 2231-2307.
9. J. Hortelano, J. C. Ruiz, and P. Manzoni, “Evaluating the usefulness of watchdogs for intrusion detection in VANETs,” in Proc. Int. Conf. Commun. Workshop, 2010, pp. 1–5.
10. 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.
11. L. Butty_an and J.-P. Hubaux, “Stimulating cooperation in selforganizing mobile ad hoc networks,” Mobile Netw. Appl., vol. 8, pp. 579–592, 2003.
12. S. Zhong, J. Chen, and Y. Yang, “Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks,” in Proc. IEEE Conf. Comput. Commun., Mar. 2003, vol. 3, pp. 1987–1997.
13. K. Paul and D. Westhoff, “Context aware detection of selfish nodes in DSR based ad-hoc networks,” in Proc. IEEE Global Telecommun. Conf., 2002, pp. 178–182.
14. M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz, “On the effect of node misbehavior in ad hoc networks,” in Proc. IEEE Int. Conf. Commun., 2004, pp. 3759–3763.
15. S. Zhong, J. Chen, and Y. Yang, “Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks,” in Proc. IEEE Conf. Comput. Commun., Mar. 2003, vol. 3, pp. 1987–1997.
16. Y. Yoo, S. Ahn, and D. Agrawal, “A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks,” in Proc. IEEE Int. Conf. Commun., May 2005, vol. 5, pp. 3005–3009.
17. 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.
18. 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.
19. Y. Zhang, W. Lee, and Y.-A. Huang, “Intrusion detection techniques for mobile wireless networks,” Wirel. Netw., vol. 9, no. 5, pp. 545–556, 2003. [Online]. Available: http://dx.doi.org/10.1023/A:1024600519144