IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 06-13
www.iosrjournals.org

Survey on Different Watchdog Systems to Deal with Selfish Nodes In MANETs

Anju Markose, Asst. Prof. Vidhya P.M
Final Year M Tech Degree Dept. of Computer Science & Engineering Sree Narayana Gurukulam College of Engineering
Dept. of Computer Science & Engineering Sree Narayana Gurukulam College of Engineering

Abstract: *The use of mobile ad hoc networks (MANETs) has been widely spread in many applications, including some mission critical applications. Security has become one of the major concerns in MANETs. Mobile Ad-hoc Networks (MANETs) assume that mobile nodes voluntary cooperate in order to work properly. MANET nodes rely on network cooperation schemes to work properly, forwarding traffic unrelated to its own use. This cooperation is a cost-intensive activity and some nodes may refuse to cooperate, leading to selfish node behaviour. Watchdogs are used to detect selfish nodes in computer networks. Different types of watchdog mechanisms are available. This paper presents a study on various watchdog mechanisms focusing on their features*
Keywords: *Selfish node; Watchdog; Isolation; MANET, Route Request, Watchdog*

I. Introduction

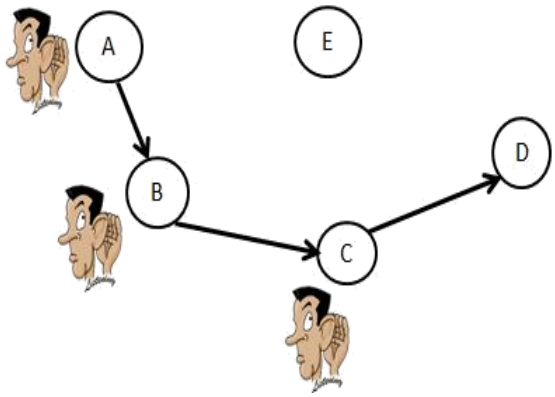
Mobile Ad Hoc Network (MANET) is a collection of mobile nodes which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANET does not depend on pre-existing infrastructure or base stations. A mobile node can become a failed node for many reasons, such as moving out of the transmission ranges of its neighbours, exhausting battery power, malfunctioning in software or hardware, or even leaving the network. A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer or any other device capable of sending and/or receiving data generated by other nodes on the network.Mobile ad-hoc networks (MANETs) are composed of mobile nodes connected by wireless links without using any pre-existent infrastructure**.**

A selfish node is one that tries to utilize the network resources for its own profit without sharing its own resources to others. Selfish node will certainly avoid itself from the routing paths because it might delay the Route Request (RREQ) packet up to the maximum upper limit time. The selfish node can participate in routing messages but it does not forward the data packets. A selfish node drops routing messages or it may modify the Route Request and Reply packets by changing time to live (TTL) value to smallest possible value.

A selfish node did not forward the data packets and hence other nodes may not be able to detect its presence when they need it. The major reason for such behaviour is low residual battery power, faulty software and hardware. Selfish node do not intend to involve itself in the network damaging activities such as Ip spoofing and so on. Hence we conclude that a selfish node is not a malicious. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data.

Watchdog helps to detect the selfish node. Working principle of watchdog is to maintain a buffer of recently sent packets and comparing each overheard packet. If the packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold, it determines that the node is misbehaving and spread the message to the source that it is a misbehaving node. The formulae for watchdog "Number of incoming message is equal to Number of outgoing message".

Figure 1 illustrates how watchdog works. Watchdog is a protocol which helps to detect the selfish node by over hearing the other nodes. Watchdog presented in all nodes in network. Node A is a source and node E is a destination. Node A forward the packets to node Watchdog present in node A overhears the neighbour node B whether it forward the packets to neighbour node C. Here node B forward the packets to node c. similarly, watchdog present in node B overhears whether node C forward the packets to node Here node D receives the packets from node Watchdog present in node C overhears the neighbour node D whether it forward the packet to E or not. Here node D did not forward the packets to destination node E.



II. Literature Review

Previously proposed methods for detecting selfish node can be classified into

(a) Audit based system
(b) Credit based systems
(c) Reputation based systems
(d) Acknowledgment based systems
(e) Collaborative based system

Audit Based System: Audit-based system that effectively and efficiently isolates both continuous and selective packet droppers. Yu Zhang and Loukas Lazo proposed a comprehensive system called Audit based Misbehaviour Detection (AMD) that effectively and efficiently isolates both continuous and selective packet droppers. The AMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioural audits. William Kozma Jr. and Loukas Lazos proposed a novel misbehavior identification scheme called REAct that provides resource-efficient account ability for node misbehaviour. REAct identifies misbehaving nodes based on a series of random audits triggered upon a performance drop.

Credit Based Systems: Credit-based systems are designed to provide incentives for forwarding packets. Buttyan and Hubaux proposed a system in which nodes accumulate credit for every packet they forward, and spend their credit to transmit their own packets. To ensure correctness, the credit counter is implemented in tamper-proof hardware. Zhong et al. proposed Sprite, in which nodes collect *receipts* for the packets they forward to other nodes. When the node has a high speed link to a Credit Clearance Service (CCS), it uploads its receipts and obtains credit. Crowcroft et al. proposed a scheme that adjusts the credit reward to traffic and congestion conditions. While credit-based systems motivate selfish nodes to cooperate, they provide no incentive to malicious nodes. Such nodes have no intended to collect credit for forwarding their own traffic. Moreover, credit-based systems do not identify misbehaving nodes, thus allowing them to remain within the network indefinitely.

Reputation Based Systems: Reputation-based systems use ratings for evaluating the trustworthiness of nodes in forwarding traffic. These ratings are dynamically adjusted based on the nodes' observed behavior. In the context of ad hoc networks, Ganeriwal and Srivastava developed a Bayesian model to map binary ratings to reputation metrics, using a beta probability density function. Jøsang and Ismail proposed a similar ranking system that utilized direct feedback received from one hop neighbours. Michiardi and Molva proposed the CORE mechanism for computing, distributing, and updating reputation values composed from disparate sources of information. Reputation-based systems use neighbouring monitoring techniques to evaluate the behaviour of nodes. Marti etal.proposed a scheme which relies on two modules, the and the *pathrater*. The watchdog module is responsible for overhearing the transmission of a successor node, thus verifying the successful packet forwarding to the next hop. The pathrater module uses the accusations generated by the watchdog module to

select paths free of misbehaving nodes. Buchegger and Le Boudec proposed a scheme called CONFIDANT, which extends the watchdog module to all one-hop neighbors that can monitor nearby transmissions (not just the predecessor node). When misbehaviour is detected, monitoring nodes broadcast alarm messages in order to notify their peers of the detected misbehaviour and adjust the corresponding reputation values. Similar monitoring techniques have also been used in. Transmission overhearing becomes highly complex in multichannel networks or when nodes are equipped with directional antennas. Neighbouring nodes may be engaged in parallel transmissions in orthogonal channels or different sectors thus being unable to monitor their peers. Moreover, operating radios in promiscuous mode for the purpose of overhearing requires up to 0.5 times the amount of energy for transmitting a message.

Acknowledgment Based Systems:

Acknowledgment based systems rely on the reception of acknowledgments to verify that a message was forwarded to the next hop. Balakrishnan et al. proposed a scheme called TWOACK, where nodes explicitly send 2-hop acknowledgment messages along the reverse path, verifying that the intermediate node faithfully forwarded packets. Packets that have not yet been acknowledged remain in a cache until they expire. A value is assigned to the quantity/frequency of unverified packets to determine misbehaviour. Liu et al. improved on TWOACK by roposing 2ACK. Similar to TWOACK, nodes explicitly send 2-hop acknowledgments to verify cooperation. Xue and Nahrsted proposed the Best-effort Fault-Tolerant Routing scheme , which relies on end-to- end acknowledgment messages to monitor packet delivery ratio and select routing paths which avoid misbehaving nodes. Awerbuch et al. proposed an on-demand secure routing protocol (ODSBR) that identifies misbehaving links. The source probes intermediate nodes to acknowledge each packet and performs a binary search to identify the link where packets are dropped. ACK-based systems also incur a high communication and energy overhead for behavioural monitoring. For each packet transmitted by the source, several acknowledgements must be transmitted and received over several hops. Moreover, they cannot detect attacks of selective nature over encrypted end-to end flows.

Collaborative Based system: Enrique Hernandez-Oralloet al. proposed 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 mobility. The disadvantage of pathrater is overhead in the transmission increases with increase the mobility

C. CONFIDANT

In Buchegger et al proposed a technique similar to watchdog and pathrater, i.e. CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad Hoc Networks). This method will detect the misbehavior node by monitoring the behavior of neighbor nodes and they will pass this information to all other nodes, the misbehavior node will not be punished. The CONFIDANT protocol contains four modules, Monitoring System, Reputation System, Trust Manager and Path Manager. Each of the modules has some specific task to perform. CONFIDANT protocol is an expansion of DSR protocol. The advantages of CONFIDANT protocol is the throughput increases, overhead of extra message is low and the disadvantage of CONFIDANT protocol is node authentication is not checked.

D. CORE

In Michiardiet. at proposed CORE (Collaborative Reputation Mechanism) to detect the selfish nodes,

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.

3. DETECTION SCHEMES

A. Watchdog

In Kachirski O et. al. , the watchdog of the node will identify the misbehaving nodes by monitoring the nearby those nodes. When a node forwards a packet to the watchdog will verifies or check whether the next node in the path will forward the packet or not. After checking if watchdog finds that if the node does not forward the packet it considered as selfish or misbehaving. The watchdog will eliminate the selfish nodes from the path and the implementation is easy. The advantage of watchdog is it can identify misbehavior node in link layer and network layer. The disadvantages of watchdog are it can't detect the misbehavior nodes in case of limited transmission power, ambiguous collision, receiver collision, minor dropping etc.

B. Pathrater

In Kachirski O et. al. , in this mechanism each node running a pathrater, each node in the network maintain a rating for all other nodes in the network. The "path metric" for every path is calculated by each node. After calculating the path metric for every path to the particular location, the path with highest metric will be chosen as the reliable path and it is decided by the pathrater. The advantage of pathrater is the throughput increases with the increase in node the mechanism also improve the coordination among nodes. It increases the cooperation among the nodes by using reputation mechanism and collaborative monitoring. The reputation values ranges from positive to negative through null. Each node computes the reputation value for all neighbor nodes.

The basic components used in the CORE mechanism are 1) reputation table and 2) watchdog mechanism.

The advantages of CORE mechanism are it will prevent the DOS attacks, it is impossible for a node to maliciously decrease another node's reputation because there is no negative rating spread between nodes. The disadvantages are CORE suffers from spoofing attack, it cannot prevent colluding nodes from distribute negative reputation

E. OCEAN

In Bansal et al proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks).OCEAN also uses the monitoring and reputation mechanism. The OCEAN layer reside on each node and have basically five components 1) Neighbor Watch 2) Route Ranker 3) Rank-Based Routing 4) Malicious Traffic Rejection and 5) Second Chance Mechanism. Each node has rating, after monitoring there is a negative or positive event is produced and uses this event to update rating of other nodes. The nodes are added to the faulty list if the rating is lower than the threshold. The advantages of OCEAN are it will distinguish the selfish and misleading nodes, network throughput increases. The disadvantage is it is failed to punish the misbehaving nodes severely.

F. 2ACK Scheme

In Manviaet. Al proposed a scheme called 2ACK scheme, it is a network layer scheme to detect the misbehavior nodes. This scheme uses a acknowledgement packet called 2ACK packet to detect the selfish nodes where the next hop node in the route will send back the 2 hop acknowledgment packet i.e. 2ACK ,this to indicate that the data packet has been received successfully. The first router from the sender not serves as the sender of 2ACK. The advantages of the schemes are it checks the confidentiality of message, increase the packet delivery ratio y detection and scheme can be added to any source routing protocol. The disadvantages are it will cause the traffic congestion on the network.

G. SORI

In He et.al proposed Secure and Objective Reputation-based Incentive (SORI) scheme. It detects the selfish nodes and encourages the packet forwarding. Reputation rate of a node is based on the packet forwarding ratio of nodes. SORI consist of three components they are neighbor monitor, reputation propagation and punishment. The packet forwarding behavior is monitored by neighbour monitor and shares this information to other nodes by use of reputation propagation. Punishment will use the information of evaluation record of a node and the threshold to make decision about the packet dropping. The advantages of the schemes are SORI is computationally efficient as compared to other methods and it reduces the communication overhead. The disadvantages are SORI does not differentiate between misbehaviour and selfish nodes and SORI has poor performance in the case of cooperation node

H. LARS

In Hu et.al proposed a scheme called Locally Aware Reputation System (LARS). This scheme finds the misbehaviour and encourages the cooperation among nodes. There are evaluator nodes they will evaluate the reputation value of the nodes. Each node will maintain the reputation value of its one hop neighbours and they will update their reputation value based on the neighbor behaviour. There is an threshold for reputation value of anode if the reputation value falls below the threshold then it is considered as misbehaving by the evaluator node. Evaluator node uses WARNING message to notify the neighbours about the Misbehaviour. The advantages of the schemes are the misbehaviour node is not completely excluded from the network, after a time out it can re-join to network such as it must increase its reputation by increase the cooperation. The disadvantages are, the power consumption of evaluator node is high and message overhead is high. Sprite in Zhonget. al proposed a scheme called sprite. In which a CCS (Credit Clearance Service) is introduced. It will determine the credit and charge of each node. Game theory methods are used to calculate the charges and credits. Each node will keep the receipt of the message its received and it will forward the receipt to the CCS. The credit of a node depends of the forwarding behavior of a node. If the next node on the path reports a valid receipt to the CCG then only the forwarding is considered as successful. A node will get more credit if it forwards the message otherwise its credit decreases. The advantages of the scheme are it can be applied to unicasting protocol and can extend to multicasting also. The disadvantages are, the collusion attack is possible and it is difficult for CCS to calculate the payment

I. Secure Incentive Protocol

In Yanchao et.al proposed SIP (Secure Incentive Protocol). SIP uses the credit as the incentive to stimulate packet forwarding. Here each mobile node has a security module and they deal with the security related functions. The credits of the node increases and decreases depend on the forwarding behaviour of the node. Whenever a node is initiating or forwarding a packet first node will pass it to sip module for processing. SIP is session based and consists of four phases, 1) Session Initiation 2) Session Key Establishment 3) Packet Forwarding And 4) Rewarding Phase. The advantages of the scheme are SIP is routing independent; it is session based rather than packet based and unauthorized access is not allowed. The disadvantage of SIP is it implemented on hardware module so each node to possess a hardware module.

J. AAS Scheme

In Gunasekaran et.al proposed Authenticated Acknowledgement Based Scheme (AAS) for preventing the selfishness in mobile Ad Hoc networks. This scheme is similar to 2ACK scheme. Which assign a fixed route of three nodes (two hops) in the opposite direction of data traffic route. A methodology must be performed by sending and receiving nodes if they wish to communicate with each other. There is a password for each transmitting packet and it will contain the data. A tag for data is formed by applying the hash function to the password. So the sending packet will contain hash value, data and tag. The advantages of the scheme are which ensure the integrity, confidentiality and authentication to the data transmitted, it increases the packet delivery ratio and throughput by increasing the selfish node detection. The disadvantages are it increases the overhead of transmission and end to end delay, AAS does not consider the weak links Detection of Selfish Nodes Using Credit Risk In Jae-Ho Choi et.al proposed the credit risk to find out the selfish
nodes. The credit risk can be described by the following equation

$$credit\ risk = \frac{expected\ risk}{expected\ value}$$

Each node will calculate the credit risk for the other nodes to which it is connected. Based on the score each

node will detect the selfish nodes. In each relocation period, the nodes will calculate the credit risk. Each node has the predefined threshold value for the credit risk. Each node will calculate the credit risk and if the calculated credit risk greater than threshold then the node is a selfish node. Expected value and expected risk are calculated based on the node specific features.

III. Comparision

Approach	**Routing Overhead**	Throughput	**FALSE Positive**	**Scalability**	**Limitations**
TWOAC	High	Increases	High	Yes	Traffic congestion
S-TWOACK Scheme	High	Increases	Low	Yes	Low packet delivery
Watchdog And Pathrater	Low	Increases	High	Yes	Ambiguous Collision,
Reputation Based Scheme	Low	Increases	Low	Yes	Node Authentication Is Not Checked
Intrusion Detection	Low	Increases	Low	Yes	Ids Is Not energy efficient
AAS scheme	High	Increases	High	Yes	It Increases the end to end delay
Ccs (Credit ClearanceService)	Low	Increases	Low	Yes	Collusion attack is possible
Cooperative Intrusion detection	Low	Increases	Low	Yes	Changed AODV implementation on every node
Secure Incentive Protocol	High	Increases	High	Yes	To Possess A hardware module
SORI (Secure And Objective Reputation Based Incentive)	Low	Increases	Low	Yes	Poor Performance
LARS	Low	Increases	Low	Yes	Not Energy Efficient

OCEAN	Low	Increases	High	Yes	Failed To punish the misbehving node

IV. Proposed Method

Combined collaborative watchdog and credit ,risk to detect the selfish node. Here we are proposing a combined scheme for the detection of selfish nodes. In the credit risk method each node will find out the selfish node individually so the detection time of the method is high. In order to reduce the detection time we are using the collaborative watchdog. Collaborative watch dog is based on contact dissemination ie if one node has a previously detected selfish node then using its watchdog it can send this information about the selfish node to other node when a contact occurs.

The detection of the contact can be easily found out using watchdog. The watchdog will overhear the packet of the neighbouring nodes. The information about the selfish nodes is called the positives. When a node receives the packet from other nodes it assumes it is a new contact, then the node will send all its all known positives to the newly contacted node. Here the node detection is performed by credit risk method and the detected information is passed to the other nodes by collaborative watch dog so the detection time will reduces.

The node has two states NONINFO and POSOITIVE, in the NONINFO state the node has no information about the selfish nodes and POSITIVE state the node has information about the selfish node

V. Conclusion

As the use of Mobile Ad hoc Networks (MANETs) has increased, the MANETs security has become more important. The selfish nodes will reduce the cooperation among the nodes in the network .Selfish nodes are a real problem for ad hoc networks since they affect the network throughput. This paper discussed several approaches for dealing with selfish nodes. Many approaches are available in the literature. But no approach provides a solid solution to the selfish nodes problem. The Credit based approach provides incentives to the well behaving nodes and just by passes the selfish nodes in selecting a route to the destination. But selfish node still enjoys services without cooperating with others. The detection and isolation mechanism isolates the selfish nodes so that they don't receive any services from the network

References

[1]. FarzanehPakzad andMarjanKuchaki Rafsanjani "Intrusion Detection Techniques for Detecting Misbehaving Nodes", in Computer and Information Science Vol. 4,-1; January 2011.
[2]. Kachirski O, Guha R. (2003). "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks", in Proceeding IEEE, (HICSS'03), pp 57.1.
[3]. Buchegger S, Le Boudec J. (2002). "Performance analysis of the CONFIDANT protocol (Cooperation of nodes fairness in dynamic ad-hoc network)", in Proceeding 3rd ACM (MobiHoc'02), pp 226–336.
[4]. Michiardi P, Molva R. (2002). "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", in International Conference on (CMS'02).
[5]. Bansal S, Baker M. (2003). "Observation-based cooperation enforcement in ad hoc networks", in Technical Paper on Network and Internet Architecture (cs.NI / 0307012). [6]. Hongxun Liu, José G. Delgado-Frias, and SirishaMedidi "USING A TWO-TIMER SCHEME TO DETECTSELFISH NODES IN MOBILE AD- HOC NETWORKS" in Proceeding of the sixth IASTED July 2-4, 2007
[6]. He, Q., Wu, D., Khosla, P., 2004. "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-Hoc Networks" in WCNC'04 IEEE Wireless Communications and Networking Conference.
[7]. Hu, J., Burmester, M., 2006. "LARS: a locally aware reputation system for mobile ad-hoc networks", in 44th annual ACM Southeast Regional Conference
[8]. S. Zhong, J. Chen, and Y. Yang, "Sprite: A Simple, Cheat-Proof, Credit- Based System for Mobile Ad-Hoc Networks", Technical Report, Yale University, July 2002
[9]. Yanchao Zhang , Wenjing Lou , Wei Liu, Yuguang Fang," A secure incentive protocol for mobile ad hoc networks" in Journal of Wireless Networks , Volume 13 Issue 5, pp. 663-678 , October 2007
[10]. M. Gunasekaran1, P. Sampath, B. Gopalakrishnan"AAS:Authenticatedacknowled gement Based Scheme For Preventing Selfish Nodes In Mobile Ad Hoc Networks "in International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009
[11]. Nasser N, Chen Y. (2007) "Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc network", in Proceeding IEEE (ICC'07), pp 1154-9
[12]. Jae-Ho Choi, Kyu-Sun Shim "Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network",inieee transactions on mobile computing, vol. 11, no. 2, february 2012
[13]. Manuel D. Serrat-Olmos, Enrique Hernández-Orallo, Juan-Carlos Cano, Carlos T. Calafate." Collaborative Watchdog to Improve the Detection Speed of Black Holes in MANETs "
[14]. Enrique Hernandez-Orallo," CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes", IEEE Transactions OnMobile Computing, Vol. 14, No. 6, 1162-1175, -June 2015.