ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

Detection of Attackers by Trusted Contact Based Watchdogs and Mitigation through Cooperative Voting in a Mobile Ad-Hoc Network

Pournami Maheshwaran[1], Sangeetha Rajagopal[2]

M.E Scholar, Department of Electronics and Telecommunication Engineering, Pillai HOC College of Engineering and Technology, Rasayani, Raigad, India[1]

Associate Professor, Department of Electronics and Telecommunication Engineering, Pillai HOC College of Engineering and Technology, Rasayani, Raigad, India[2]

ABSTRACT: Mobile Ad-hoc network (MANET) is built from various number of mobile nodes. Regardless of any infrastructure, it can be moved to anywhere and at anytime. MANETs use wireless connections to connect various networks, without any fixed infrastructure or any centralized administration. The network communication can be deliberately disrupted by malicious or compromised nodes along the communication path .Due to this nature of MANET, Ad hoc networks are open to different types of security attacks. So protecting the mobile ad-hoc network from malicious attacks is very important and challenging issue. In this paper we address the problem of packet forwarding misbehavior and propose a mechanism to detect, identify and mitigate the black and gray hole attacks. Our technique is capable of identifying the attacks by finding chain of cooperating malicious nodes which drop a significant fraction of packets. We also propose a Voting Based Attack Mitigation technique to mitigate the black hole and gray hole attacks. The simulation results are compared with different situation and attempt to improve the performance of AODV protocol for the parameters like Packet Delivery Ratio and Throughput.

KEYWORDS: Mobile Ad-hoc Network, Black Hole Attack and Gray Hole Attack.

I. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) and opportunistic and delay tolerant systems (DTNs) are the two fundamental advances that are considered as the center for VANETs or mobile social networks. A contact is characterised when there is a chance of transmission between a pair of nodes so that the packets are conveyed on time. The nodes that are inside the correspondence range can speak with each other without any problem whenever a contact occurs. Hence , in view of the contact between the nodes, the participation on these systems is possible. As it is a cost concentrated action for portable nodes, it is difficult to support this collaboration. Usually nodes display a narrow minded conduct in which it doesn't demonstrate any ability to forward the packets for others. In order to spare their own particular assets, a few nodes decline to forward other nodes' bundles which is seen as selfishness.

A supporting framework is not needed to acknowledge end-to-end correspondences in a wireless ad-hoc network. Nodes depend on the foundation of multi hop routes in order to beat the constraints of their limited correspondence range. Intermediate nodes are in charge of handing off packets from the source to the destination in this pattern.[3]

In certain strategic systems in wireless ad-hoc networks packets are not forwarded safely. We can't expect safe and secure transmissions in such threatening situations. Unattended gadgets can get to be traded off and drop transit traffic with a specific end goal to degrade the system execution. Also, selfish clients may misconfigure their gadgets to deny

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

sending movement with a specific end goal to save vitality. This sort of conduct is ordinarily termed as node misbehaviour (AMD)

There are two basic methodologies to manage the selfish nodes. The identification and prohibition methodology are the two fundamental procedures to handle selfish nodes.

The packets that are sent by another node to a particular node are not re-transmitted. As a result the packet is lost and this is how the selfish nodes work. In order to forward the packets efficiently without any drop, it is exceptionally important to distinguish such selfish nodes rapidly and precisely. Watchdogs are the appropriate technique to locate selfish and malicious nodes. Basically, watchdog frameworks catch remote activity and break down it to choose whether neighbour nodes are behaving in a selfish manner or not [16]. The location of a selfish node by a watchdog is set apart as a positive recognition and when a non selfish node is distinguished, it is set apart as negative detection. There are chances that the watchdogs may come up short in the discovery strategy and therefore create false positives and false negatives which can genuinely corrupt the general conduct of the framework.

The intrusion detection systems that has been proposed so far for self-arranging remote systems administration frameworks like VANETs has watchdog as the essential segment. Intrusion detection systems (IDS) goes for observing the movement of the different nodes in the system with a specific end goal to distinguish mischievous activities. An essential block in the development of such frameworks is the watchdog, a segment utilized for the detection of selfish nodes and malicious attackers. At the point when a node advances a packet, the watchdog confirms that the following node in the way additionally advances the packet. It does this by listening indiscriminately to the following node's transmissions. In the event that the following node does not forward the packet, then it is acting up. Results given by watchdogs are exploited by other reputation systems, as on account of the Pathrater and Routeguard arrangements. Such frameworks then confine and/or rebuff misbehaving nodes by diminishing their trustability rates. An intrusion is the outcome of an assault that succeeds in the abuse of a current defenselessness. The watch dog as the essential block of an IDS arrangements. [3]

In this paper, we are categorizing nodes into trusted and normal. The trusted nodes is not having possibilities for malicious or selfish node. The report on trusted nodes as selfish will not be considered in detection process. So false positive probability will be reduced i.e., trusted nodes can't be reported as selfish.
While making the data routing, the trusted nodes gets higher preference than normal nodes. So packets will be most probably delivered by trusted nodes. So possibilities for malicious action will be less. We adopt a reputation based trust route mechanism with the help of a contact based watchdog to identify the selfish and malicious node. We also detect the black hole and gray hole attacks and then reduce the packet drops by attackers through a voting based mitigation process.

II. RELATED WORK

CoCoWa

A collaborative approach known as Collaborative contact-based watchdog (CoCoWa) has been proposed by the authors in order to quickly propagate awareness regarding the diffusion of local selfish nodes whenever a contact occurs. As appeared in the paper [1], this cooperative approach diminishes the time and expands the accuracy when recognizing the selfish nodes. Execution assessment diminish the time and enhance the adequacy of identifying selfish nodes, decreasing the unsafe impact of false positives, false negatives and malicious nodes. CoCoWa depends on the dissemination of the known positive and negative identifications. At the point when a contact happens between two collaborative nodes, the dispersion module transmits and forms the positive (and negative) recognitions. We have assessed the impact of false positives and false negatives. Thus the effect of malicious and collusive nodes can be reduced.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

Audit Based Misbehaviour

The Audit-based Misbehavior Detection (AMD) framework incorporates notoriety administration, trustworthy route revelation, and distinguishing proof of making misbehaving nodes in light of behavioral reviews. AMD assesses node conduct on a per-packet premise, without utilizing vitality costly catching procedures or serious affirmation plans. Also, AMD can distinguish specific dropping attacks regardless of the fact that end-to-end activity is scrambled and can be connected to multi-channel systems or systems comprising of hubs with directional radio wires. AMD, a far reaching misbehaviour detection and moderation framework which coordinates three basic capacities: notoriety administration, course revelation, and ID of getting out of hand hubs by means of behavioral reviews. The procedure of distinguishing acting up nodes are shown as R'enyi-Ulam diversions and determined asset effective recognizable proof methodologies.AMD recoups the system operation regardless of the fact that an expansive part of nodes is getting out of hand at an altogether bring down correspondence cost. In addition AMD can recognize particular dropping assaults over end to-end encoded activity streams[2].

Light Weight Sybil Attack

A Sybil attacker [3] can either make more than one personality on a solitary physical gadget keeping in mind the end goal to dispatch an organized attack on the system or can switch characters so as to debilitate the recognition process, in this manner advancing absence of responsibility in the system. In this exploration, we propose a lightweight plan to distinguish the new personalities of Sybil assailants without utilizing brought together trusted outsider or any additional equipment, for example, directional receiving wires or a land situating framework. Through the assistance of broad recreations and real world testbed tests, we can exhibit that our proposed plan identifies Sybil personalities with great exactness even within the sight of versatility. We affirmed qualification of genuine new nodes and new noxious personalities method of reasoning through reenactments and using a real world testbed of Sun SPOT sensors. Likewise the different variables influencing the location exactness, for example, system associations, bundle transmission rates, hub thickness, and node speed are demonstrated.

Improving Selfish Node Detection

This paper proposes a synergistic watch dog taking into account contact spread of the distinguished selfish nodes. At that point, we acquaint a scientific model which assess the identification time and the expense of this community approach. Numerical results demonstrate that our community oriented watch dog can drastically diminish the general location time with a decreased overhead. Numerical results demonstrate that a collective watchdog can decrease the general location time with a diminished expense in term of message overhead. This diminishment is extremely huge when the guard dog location adequacy is low. Moreover, this decrease can be gotten even with a moderate level of joint effort [4].

Impact of Node Selfishness

In this paper, the selfish practices of nodes influence the execution of DTN multicast are explored.Two normal multicast transferring plans, in particular, two-bounce handing-off and plague transferring, and think about their execution regarding normal message transmission postponement and transmission cost are considered. In particular, the message conveyance process under narrow minded practices are demonstrated by a 3-D nonstop time Markov chain; under this model, shut structure equations are determined for the message transmission postpone and cost. At that point, the precision of the proposed Markov chain model is assessed by contrasting the hypothetical results and the reproduction results acquired by mimicking the message scattering under both two-bounce and pestilence transferring with various system sizes and versatility models. As far as various selfish practices are considered, the individual narrow-mindedness of not sending messages builds the message transmission postpone and cost, which is detrimental to the DTN multicast, while the individual self-centeredness of not replicating messages and the social childishness expand the message transmission defer however lessen the transmission cost. Especially in multicast applications

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

immediately necessity, they can be utilized to lessen the framework cost. As far as various transferring plans in the multicast, the selfish behaviours are demonstrated which influence pestilence handing-off more than two-hop transferring [5].

\

Efficient and Secure Cooperation Incentive Protocol

Secure collaboration is proposed motivating force convention that uses general society key operations just for the main parcel in an arrangement and utilization of the lightweight hashing operations in the following bundles, so that the overhead of the bundle arrangement focalizes to that of the hashing operations. Hash chains and keyed hash qualities are utilized to accomplish installment non revocation and ruin free riding assaults. Secure participation impetus convention with constrained utilization of open key cryptography for multihop remote systems have been proposed. Security examination and execution assessment show that the proposed convention is secure and the overhead is exceptional to the general population key-based motivator conventions on the grounds that the proficient hashing operations overwhelm the nodes' operations.

Also, the normal parcel overhead is not exactly those of general society key-based conventions with high likelihood because of truncating the keyed hash values. General society key operations are required just for the principal parcel and the productive hashing operations are utilized as a part of the following bundles, so for a progression of bundles, the overwhelming overhead of the main bundle vanishes and the general overhead merges to that of the lightweight hashing operations. Security investigation and execution assessments have exhibited that ESIP can secure the installment and enhance the system execution altogether in light of the fact that the hashing operations rule the hubs' operations. For a progression of two parcels, ESIP has lower cryptographic deferral and vitality than DSA and RSA-based conventions, and for a progression of 13 parcels, ESIP requires around 10 percent of the cryptographic postponement and vitality in DSA and RSA-based conventions [6].

Heterogeneous Opportunistic Networks

Heterogeneity of individual sets contact designs assumes an urgent part in deciding the total between contact times measurements, and that concentrating on the last just can deceive. In this paper the reliance between the appropriations of i) individual pairs inter-contact times, ii) the rates of individual pairs inter-contact times, and iii) the total inter-contact times, in mobile opportunistic networks have been explored through an investigative model. In heterogeneous systems (i.e., when not all the pair distributions are the same), substantial tailed total conveyances can seem beginning from exponentially dispersed individual pairs inter-contact times have been demonstrated. In this way, the total distribution is not representative, by and large, of the individual pair distributions, and that concentrating on the previous to check properties that rely upon the last can in this way be misleading [7].

Selfish Check Negotiation Protocol

SCNP Selfish Check Negotiation Protocol is presented to permit nodes to arrange for joint effort at whatever point conceivable. Likewise examine the "effect" of being selfish and unselfish, particularly on collaborative applications, and system correspondence execution.A selfish check arrangement convention have been proposed to allow nodes to arrange for cooperation at whatever point conceivable. This methodology can enormously decrease route failures, packet losses, and control overhead [8].

Evaluating the usefulness of watchdog

The watchdog strategy is a determination system valuable to recognize directing disruption attacks in ad hoc networks. It is autonomous of the convention and innovation utilized, and afterward a legitimate device for intrusion detections on any ad hoc networks, for example, VANETs. The most important issues of this strategy are essentially identified with the presence of false positive and false negative detection events. A calculation to control these two issues by presenting what we called the tolerance threshold and devaluation mechanisms have been proposed [9].

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

Vulnerabitlity towards Node Selfishness

The execution of two well known information handing-off options, the unhindered and two-hop relay schemes, when nodes act selfishly while sending information have been evaluated. The execution point of preference of unhindered relaying over two-hop relaying declines both with the number of selfish nodes and the power of their selfishness, regardless of whether nodes concede from transferring deterministically or probabilistically.The defenselessness of the two relaying schemes to node selfishness are utilized additionally to drive remediation activities against it [10].

III. DETECTION AND IDENTIFICATION OF SELFISH AND MALICIOUS NODES

CoCoWa Architecture

The Local watchdog has mainly two fuctions:
1) Selfish nodes' detection and
2) New contacts detection.

The following events are generated when the watchdog detects a selfish neighbour node :
Detection of selfish node by watchdog generates PosEvt (positive event)
Detection of non selfish nodes by watchdog generates NegEvt (negative event) .
The watchdog does not overhear enough messages if the contact time is very low.At that time, enough information about a node is not detected and it generates NoDetEvt (no detection event)

A new contact can be detected when the neighbourhood packet overhears. An event is generated to the network information module when packets from a new node are overheard by the watchdog and are assumed to be a new contact by them.
The positive and negative detections are transmitted and received by the Diffusion Module.

The transmission of positive detections can be done with a low overhead as the number of selfish nodes is low as compared to the total number of nodes and so there is an issue of diffusion of information due to this.

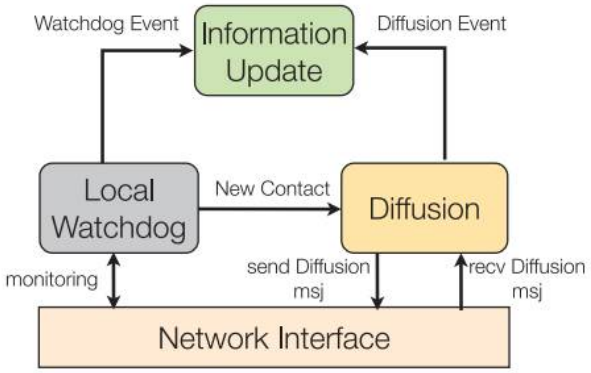

Fig 1.CoCoWa Architecture [1]
Another key issue is the updation and consolidation of the information..This is the function of the Information Update Module.

A node can have the following internal information about another nodes :
NoInfoState, Positive state and Negative state.

1) When there is no information about a node, a NoInfoState occurs.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

2) When a node is selfish, a Positive state occurs.
3) When a node is not selfish, a Negative state occurs.

A node can have both direct information from the local watchdog and indirect information from neighbour nodes. The state of the node is updated whenever the positive and negative events are received from the local watchdog and diffusion modules. Hence, we can say CoCoWa[1] is event driven.

Thus the implementation of this mechanism is straight forward.

Detection

Initially reputation value has to be calculated. Based on the reputation value, we fix a threshold value. The nodes above the value are trusted nodes. Below the threshold are non trusted nodes. Now, the threshold trusted node has a possibility for an attacker. While forwarding the packets, the malicious node will drop the packets. At that time, the trusted nodes will report about the attacker formed in the past to the network.

The reports from the trusted nodes only will be accepted while the reports from the non trusted nodes will not be accepted. Trusted nodes will monitor its neighbour using CoCoWa. Thus the trusted nodes will optimize and create the reports and thus the probability of false negatives and false positives is generated.

The source will calculate the probability values and after that it can find the attacker in that path. Thus, the detection part is done.

Identification :

In this paper we tackled two types of routing attacks namely Gray hole attack and Black hole attack which exhibits packet forwarding misbehavior. In a black hole attack malicious node (called black hole) replies to every route request by falsely claiming that it has a fresh enough route to the destination. In this way all the traffic of the network are redirected to that malicious node which then dumps them all. A gray hole attack is a variation of black hole attack, where an adversary first behave as an honest node during the route discovery process, and then silently drops some or all of the data packets sent to it for further forwarding even when no congestion occurs. Detection of gray hole attack is harder because nodes can drop packets partially not only due to its malicious nature but also due to overload, congestion or selfish nature. Here, we have identified black hole and gray hole attacks using CoCoWa. If the number of packets dropped is 100%, then the malicious node would be detected as a black hole attack and if the number of packets dropped is 50%, then the malicious node would become gray hole attack.

In the identification part, we are dividing the network using reputation mechanism. The nodes which have reputation will be trusted and the others would be non trusted. Here we are going to accept reports only from trusted nodes. We won't accept the false reports from the non trusted nodes. The compromised nodes may have a low reputation value and so reports from them are not acceptable. Due to this, they are categorized into non trusted nodes. The reports from the non trusted nodes will not be acceptable. Hence, we can detect the selfish nodes accurately as well as identify the black hole and gray hole attacks. This, in turn, reduces the packet mishandling in the network.

Voting Based Attack Mitigation

In this paper we present a mechanism capable of detecting and removing the malicious nodes launching two types of attacks ie. Gray Hole Attack and Black Hole Attack. Our approach consists of an algorithm which works as follows.The source node sends route discovery packet. After receiving route request packet RREQ, the destination will send route reply packets RREP. Alongwith the route reply packet, we will add another table in which malicious nodes' should be added. Each and every node which are sending the route reply packet will add the malicious node details. After receiving RREP, the source node will set a threshold value and the source will count the number of votes for each and every node. The nodes which have the value greater than the threshold value will be the attacker. It finds the path for destination. After sending the discovery packets, the receiver node sends route reply about the path details or destination. Alongwith the route reply, we use voting process. Every node will vote. The nodes will vote about an attacker. Source will fix one threshold value. If the number of votes exceed the threshold value, then the node will be

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

the attacker. So the source node will eliminate the attacker from the routing path and afterwards, it can send the packets through secure path.

Our methodology is based on the assumption that a neighborhood of any node in the ad hoc network has more trusted nodes than malicious nodes. Source node gets vote of one node's neighbors about the maliciousness. According to the votes of neighbors, starts counter for malicious node in Find Malicious table. If votes of neighbors about maliciousness exceeds
from a limit, source enters that node in Gray/Black hole table and finds a new route to destination.Also announces to the network that node is a malicious one.

Thus, Black Hole and Gray Hole Attacks can be eliminated.

Simulation Results:
Our simulation results show the difference in the network performance when the attacks are detected and when the attacks are mitigated with the help of graphs which are :
1)Throughput vs receivers and
2)Packet delivery ratio vs receivers.

Performance Parameters :
Throughput : The number of bytes received above transmitted per second is known as Throughput.

Packet Delivery Fraction (PDF) : The fraction of the count of delivered data packets at the destination node is called Packet Delivery Fraction

In the detection part, all the attackers are not detected. So compromised nodes are not identified and packet mishandling is very high. The false reports are generated and hence, packet deliver ratio and throughput would be low compared to identification and mitigation sections.
In the mitigation part, we are not allowing the attackers to misbehave with the packets. By voting process, we are aware about the attackers. We can eliminate the attackers from the routing path and we can successfully transmit the packets from the source to the destination. Hence, a secure transmission of packets is possible because of the mitigation of black hole and gray hole attacks..
The simulation results show the comparison between the detection and mitigation part. The packet delivery ratio is higher in the mitigation part than the detection part as the packet mishandling is v less when the black hole and gray hole attacks are mitigated. As a result of this the packets are successfully transmitted from the source to the destination. Hence the throughput is also high in the mitigation part.
Thus the following simulation results show that network performance increases when the black hole attacks and gray hole attacks are mitigated.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

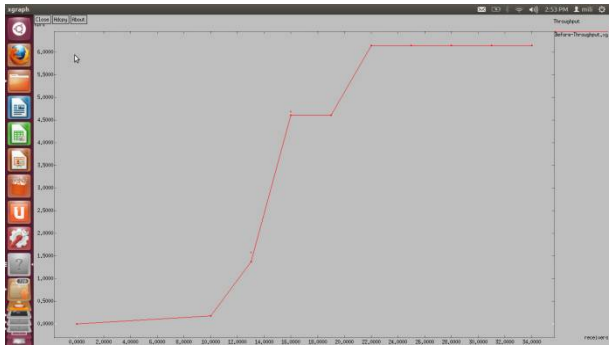

Fig 2.Graph for Throughput vs Receivers when the attacks were detected

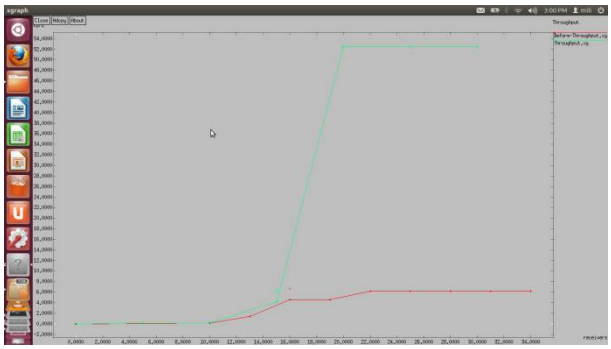

Fig 3.Graph for Throughput vs Receivers when the attack was mitigated

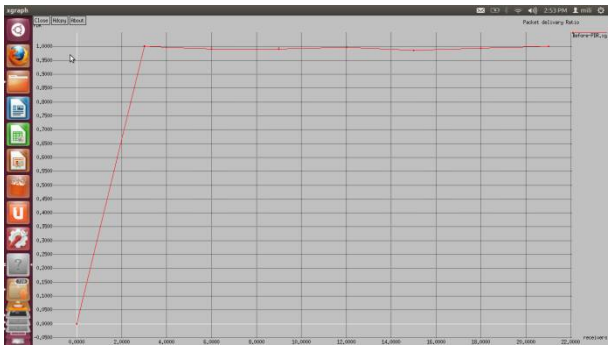

Fig4.Graph for Packet delivery ratio vs Receivers when the attacks were detected

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

Fig5.Graph for Packet delivery ratio vs Receivers when the attack was mitigated

IV. CONCLUSION

. In this paper we have studied the CoCoWa[1] architecture which is used for the detection of selfish and malicious nodes and then based on the packet drops, we proposed a feasible solution for identification of attacks and removal of black and gray hole attacks in AODV protocol.

There are some methods which are already implemented to solve this mitigation problem of attack. Because of lack of any centralized authentication or fixed infrastructure, the MANET security is the biggest challenge for the wireless network. The network suffers from various security attacks as the wireless link can be accessed by all. In this paper, we have proposed a solution to detect, identify and eliminate the attacks using voting based attack mitigation technique using AODV routing protocol. The proposed algorithm is applicable for detection and elimination of the gray hole and black hole attacks and the performance parameters like throughput, and packet delivery ratio are compared between detected and mitigated scenarios in the AODV protocol .

REFERENCES

[1] Enrique Hernandez-Orallo, Manuel David Serrat Olmos, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni,**''CoCoWa: A Collaborative contact-based watchdog for detecting selfish nodes,''** IEEE Trans. on Mobile Computing, vol. 14, no. 6, Jun 2015.
[2] Y. Zhang, L. Lazos, and W. Kozma, **"AMD: Audit-based misbehavior detection in wireless ad hoc networks,"** IEEE Trans. Mobile Comput., vol. PP, no. 99,2013.
[3] 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.
[4] E. Hernandez-Orallo, M. D. Serrat, J.C. Cano, C. M. T. Calafate, and P. Manzoni, **''Improving selfish node detection in MANETs using a collaborative watchdog,''**IEEE Comm. Lett., vol. 16, no. 5,pp. 642-645, May 2012.
[5] Y. Li, G. Su, D. Wu, D. Jin, L. Su, and L. Zeng, **''The impact of node selfishness on multicasting in delay tolerant networks,''** IEEE Trans. Veh. Technol., vol. 60, no. 5, pp. 2224-2238, Jun. 2011.
[6] M. Mahmoud and X. Shen, **"ESIP: Secure incentive protocol with limited use of public-key cryptography for multihop wireless networks,"** IEEE Trans. Mobile Comput., vol. 10, no. 7, pp. 997–1010, Jul. 2011.
[7] A. Passarella, and M. Conti, **"Characterising aggregate intercontact times in heterogeneous opportunistic networks,"** in Proc.10th Int. IFIP TC 6 Conf. Netw., 2011, pp. 301–313.
[8] C. Toh, D. Kim, S. Oh, and H. Yoo, **''The controversy of selfish nodes in ad hoc networks,''** in Proc. Adv. Commun. Technol., Feb. 2010, vol. 2, pp. 1087–1092.
[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] M. Karaliopoulos, **''Assessing the vulnerability of DTN data relaying schemes to node selfishness,''** IEEE Commun. Lett.,vol. 13, no. 12, pp. 923-925, Dec. 2009.
[11] Q. Li, S. Zhu, and G. Cao, **"Routing in socially selfish delay tolerant networks,"** in Proc. IEEE Conf. Comput. Commun, 2010, pp. 857–865.
[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] S. Eidenbenz, G. Resta, and P. Santi, **"The COMMIT protocolfor truthful and cost-efficient routing in ad hoc networks withselfish nodes,"** IEEE Trans. Mobile Comput., vol. 7, no. 1,pp. 19–33, Jan. 2008.
[14] P. Hui, J. Crowcroft, and E. Yoneki**, "Bubble rap: social-based forwarding in delay tolerant networks,"** in Proc. 9th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2008, pp. 241–250.
[15] 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.