ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Detection of Selfish and Malicious Nodes in MANET Using Watchdog Mechanism

Arul Jothi .T , Ramya Cauvery . D

Department of computer science and engineering,
Mookambigai College of engineering,
Pudukkottai,
India.
baruljothi.90@gmail.com

***Abstract*— Cooperative networking is currently receiving significant attention as an emerging network design strategy for future mobile wireless networks. Successful cooperative networking can prompt the development of advanced wireless networks to cost-effectively provide services and applications in contexts such as vehicular ad hoc networks (VANETs) or mobile social networks. Mobile Ad-hoc Network is acontinuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. In this, a new scheme Collaborative Contact based Watchdog (CoCoWa) have been introduced for detecting selfish and malicious nodes. A common technique to detect this selfish and malicious behaviour is network monitoring using local watchdogs. A node's watchdog consists on overhearing the packets transmitted and received by its neighbours in order to detect anomalies, such as the ratio between packets received to packets being retransmitted. By using this technique, the local watchdog can generate a positive (or negative) detection in case the node is acting selfish (or not). It proposes a work based on the combination of a local watchdog and the diffusion of information when contact occurs between pairs of nodes.**

***Keywords:* Wireless networks, MANETs, selfish nodes, malicious nodes, Neighbor Discovery Protocol.**

I. INTRODUCTION

MANETS are used in various contexts like intelligent Transportation systems, mobile social networks, emergency deployment, etc. In a MANET, nodes can freely move around while communicating with each other. These networks may under-perform in the presence of nodes with a selfish behavior, particularly when operating under energy constraints. A selfish node will typically not cooperate in the transmission of packets, seriously affecting network performance. Although less frequent, nodes may also fail to cooperate either intentionally (a malicious behavior) or due to faulty software or hardware.

The impact of node selfishness on MANETs has been studied in credit-payment scheme. In credit-payment scheme it is shown that when no selfishness prevention mechanism is present, the packet delivery rates become seriously degraded, from a rate of 80 percent when the selfish node ratio is 0, to 30 percent when the selfish node ratio is 50 percent. The number of packet losses is increased when the selfish node ratio increases. A more detailed study shows that a moderate concentration of node selfishness (starting from a 20 percent level) has a huge impact on the overall performance of MANETs, such as the average hop count, the number of packets dropped, the offered throughput, and the probability of reachability. In DTNs, selfish nodes can seriously degrade the performance of packet transmission. For example, in two-hop relay schemes, if a packet is transmitted to a selfish or malicious node, the packet is not re-transmitted, therefore being lost.

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

Additionally, CoCoWa is also effective in opportunistic networks and DTNs, where contacts are sporadic and have short durations, and where the effectiveness of using only local watchdogs can be very limited. In short, the combined effect of collaboration and reputation can reduce the detection time while increasing the global accuracy using a moderate local precision watchdog. The cooperation on these networks is usually contact based. Mobile nodes can directly communicate with each other if a contact occurs (that is, if they are within communication range). Supporting this cooperation is a cost intensive activity for mobile nodes. Thus, in the real world, nodes could have a selfish behavior, being unwilling to forward packets for others. Selfishness means that some nodes refuse to forward other nodes' packets to save their own resources.

Another source of problems for cooperative approaches is the presence of colluding or malicious nodes. Malicious nodes are hard to detect using watchdogs, as they can intentionally participate in network communication with the only goal to hide their behavior from the network. Thus, since these nodes may be present on the network, evaluating their influence becomes a very relevant matter. This collaborative approach extends the previous approaches to also cope with malicious nodes using a reputation scheme.

A Collaborative Contact-based Watchdog (CoCoWa) has been introduced as a new scheme for detecting selfish and malicious nodes that combines local watchdog detections and the dissemination of this information on the network. If one node has previously detected a selfish or malicious node it can transmit this information to other nodes when a contact occurs. This way, nodes have second hand information about the selfish and malicious nodes in the network. The goal of CoCoWa is to reduce the detection time and to improve the precision by reducing the effect of both false negatives and false positives.

The diffusion of information about positive or negative detections of selfish and malicious nodes introduces several issues about the reputation of the neighbor nodes. The first issue is the consolidation of information, that is, the trust about neighbor's positive and negative detections, especially when it does not match with the local watchdog detection.

Formally, a network consists of N wireless mobile nodes, with C collaborative nodes and S selfish nodes. Initially, the collaborative nodes have no information about the selfish nodes. A collaborative node can have a positive when a contact occurs in the following way:

- *Selfish contact*: one of the nodes is the selfish node. Then, the collaborative node *can* detect it using its watchdog and have a positive about this selfish node. Nevertheless, a contact does not always imply detection. To model this fact, a probability of detection (pd) has been introduced. This probability depends on the effectiveness of the watchdog and the type of contact (for example if the contact time is very low, the watchdog does not have enough information to evaluate if the node is selfish or not).
- *Collaborative contact*: both nodes are collaborative. Then, if one of them has one or more positives, it *can* transmit this information to the other node; so, from that moment, both nodes have these positives. As in the *selfish contact* case, a contact does not always imply a collaboration. It can be modelled with the probability of collaboration (pc). The degree of collaboration is a global parameter of the network to be evaluated. This value is used to reflect that either a message with the information about the selfish nodes is lost or that a node temporally does not collaborate (for example, due to a failure or simply because it is switched off). In real networks, full collaboration (pc = 1) is almost impossible.

In order to evaluate the efficiency of CoCoWa, an analytical performance model has been introduced. The network can be modeled as a continuous time Markov chain (CTMC) and derive expressions for obtaining the time and overhead (cost) of detection of selfish and malicious nodes under the influence of false positives and false negatives. In general, the analytical evaluation shows a significant reduction of the detection time of selfish and malicious nodes with a reduced overhead when comparing CoCoWa against a traditional watchdog. The impact of false negatives and false positives is also greatly reduced. Finally, the pernicious effect of malicious nodes can be reduced using the reputation detection scheme. We also evaluate CoCoWa with real mobility scenarios using well known human and vehicular mobility traces. These experimental results confirm that CoCoWa approach is very efficient.

Characterizing inter-contact times (or inter-meeting times) between pairs of nodes is essential for analyzing the performance of contact-based protocols in cooperative networking. The inter-contact times distribution is obtained by Aggregating the individual pair distribution of all combinations of pairs of nodes in the network. The individual pair distribution is defined as the distribution of the time elapsed between two consecutive contacts between the same pair of nodes

II. Neighbor Discovery Protocol(NDP)

In this section, a wormhole-resilient secure neighbor discovery protocols (NDPs for short) has been presented. It describes a neighborhood discovery protocol

(NHDP) for a mobile ad hoc network (MANET) [RFC2501]. This protocol uses a local exchange of HELLO messages so that each router can determine the presence of, and connectivity to, its 1-hop and symmetric 2-hop neighbors. Messages are defined and sent in packets according to the specification [RFC5444].

1-hop neighborhood information is recorded for use by MANET routing protocols to determine direct (1-hop) connectivity to neighboring routers. 2-hop symmetric neighborhood information is recorded so as to enable MANET routing protocols to employ flooding reduction techniques, e.g., to select reduced relay sets for efficient network-wide traffic dissemination. 1-hop and symmetric 2-hop neighborhood information is recorded in the form of Information Bases. These are available for use by other protocols, such as MANET routing protocols that require information regarding the local network connectivity. This protocol is designed to maintain the information in these Information Bases even in the presence of a dynamic network topology and wireless communication channel characteristics. The set of neighbor routers of a given MANET router may be continuously changing, often due to router mobility or a changing physical environment in which the MANET is located. There is typically no information from lower layers that would enable an IP routing protocol to detect and, as appropriate, react to such changes. Such changes can often take place on a short timescale, such as of the order of seconds, requiring MANET routing protocols to act rapidly to ensure suitable convergence properties.

MANET routing protocols, for example [RFC3626] and [RFC5449], often employ relay set reductions in order to conserve network capacity when maintaining network-wide topological information, with calculation of these reduced relay sets employing up to two hop information.The neighborhood discovery protocol provides continued tracking of neighborhood changes, link bi-directionality, and local topological information up to two hops. Combined, this allows a MANET routing protocol access to information describing establishment/disappearance and provides the necessary topological information for reduced relay set selection and other purposes. Neighbor discovery is a fundamental requirement and need be done frequently in Mobile Ad-hoc networks (MANETs) with floating node mobility. In hostile environments, neighbor discovery is vulnerable to the wormhole attack by which the adversary uses secret wormhole links to make distant nodes falsely accept each other as a neighbor. The wormhole attack may lead to many undesirable consequences and cannot be solved by cryptographic methods.

A wormhole attack is a particularly severe attack on MANET routing where two attackers connected by a high-speed off-channel link called the wormhole link. The wormhole link can be established by using a network cable and any form of ―wired link technology or a long-range wireless transmission in a different band. The solution consists of four secure wormhole resilient Neighbor Discovery protocols. The first protocol B-NDP involves two nodes in each instance of neighbor discovery and it identifies fake neighbors, while the second protocol DV-NDP requires three nodes and this protocol detects wormhole attacks. DV-NDP dramatically improves the wormhole resilience of B-NDP at the cost of decreasing the probability of two true neighbors successfully discovering each other. The third protocol SDV-NDP turns DV-NDP into a deterministic wormhole-resilient protocol with little modification and probability estimation. By the last protocol MA-NDP, we show how to accommodate floating node mobility in UANs during the execution of B-NDP, DV-NDP, or SDV-NDP and it predicts neighboring relationships. All of our schemes can provide strong resilience to the wormhole attack.

• ***True neighbors*****:** Two nodes are called *true neighbors* if they are in each other's transmission range and both have authentic public/private keys issued by the authority.

• ***Fake neighbors:*** Two nodes are called *fake neighbors* if they are not true neighbors but can communicate via a wormhole link invisible to them.

• ***Pf*****:** It is defined as the probability that a node establishes a neighboring relationship with a fake neighbor after a complete NDP execution.

• ***Ps*****:** It is defined as the probability that two true neighbors can establish neighboring relationship.

The goal of this section is to model the behavior of the different modules of CoCoWa architecture. The local watchdog is modeled using three parameters: the probability of detection pd, the ratio of false positives pfp, and the ratio of false negatives pfn. The first parameter, the probability of detection (pd), reflects the probability that, when a node contacts another node, the watchdog has enough information to generate a PosEvt or NegEvt event. This value depends on the effectiveness of the watchdog, the traffic load, and the mobility pattern of nodes. For example, for opportunistic networks or DTNs where the contacts are sporadic and have low duration, this value is lower than for MANETs. Furthermore, the watchdog can generate false positives and false negatives.). CoCoWa is event driven, so the state of a node is updated when the PosEvt or NegEvt events are received from the local watchdog and diffusion modules.

III. ARCHITECTURE OVERVIEW

A selfish node usually denies packet forwarding in order to save its own resources. This behavior implies that a selfish node neither participates in routing nor relays data packets. Malicious effect can even be more harmful, since these nodes try to intentionally disturb the correct behaviour of the network. A common technique to detect this selfish and malicious behavior is network monitoring using local watchdogs. A node's watchdog consists on overhearing the packets transmitted and received by its neighbors in order to detect anomalies, such as the ratio between packets received to packets being retransmitted. By using this technique, the local watchdog can generate a positive (or negative) detection in case the node is acting selfishly or maliciously (or not).

COCOWA is based on the combination of a local watchdog and the diffusion of information when a contact between pairs of nodes occurs. A contact is defined as an opportunity of transmission between a pair of nodes (that is, two nodes have enough time to communicate between them). If there is only one selfish or malicious node, then initially no node has information about the selfish or malicious node. When a node detects a selfish or malicious node using its watchdog, it is marked as a positive, and if it is detected as a non selfish node or non malicious node, it is marked as a negative. Later on, when this node contacts another node, it can transmit this information to it; so, from that moment on, both nodes store information about these positive (or negative) detections. Therefore, a node can become aware about selfish and malicious nodes directly (using its watchdog) or indirectly, through the collaborative transmission of information that is provided by other nodes.

Under this scheme, the uncontrolled diffusion of positive and negative detections can produce the fast diffusion of wrong information, and therefore, a poor network performance.

The functional structure of CoCoWa consists of three main components.

The Local Watchdog has two functions: the detection of selfish and malicious nodes and the detection of new contacts. The local watchdog can generate the following events about neighbor nodes: PosEvt (positive event) when the watchdog detects a selfish or malicious node, NegEvt (negative event) when the watchdog detects that a node is not selfish or not malicious, and NoDetEvt (no detection event) when the watchdog does not have enough information about a node (for example if the contact time is very low or it does not overhear enough messages). The detection of new contacts is based on neighborhood packet overhearing; thus, when the watchdog overhears packets from a new node it is assumed to be a new contact, and so it generates an event to the network information module.

The Diffusion module has two functions: the transmission as well as the reception of positive (and negative) detections. A key issue of our approach is the diffusion of information. As the number of selfish and malicious nodes is low compared to the total number of nodes, positive detections can always be transmitted with a low overhead. However, transmitting only positive detections has a serious drawback: false positives can be spread over the network very fast. Thus, the transmission of negative detections is necessary to neutralize the effect of these false positives, but sending all known negative detections can be troublesome, producing excessive messaging or the fast diffusion of false negatives.

Finally, when the diffusion module receives a new contact event from the watchdog, it transmits a message including this information to the new neighbor node. When the neighbor node receives a message, it generates an event to the network information module with the list of these positive (and negative) detections.

Updating or consolidating the information is another key issue. This is the function of the Information Update module. A node can have the following internal information about other nodes: No Info state, Positive state and Negative state. A No Info state means that it has no information about a node; a Positive state means it believes that a node is selfish or malicious, and a Negative state means it believes that a node is not selfish and not malicious. A node can have direct information (from the local watchdog) and indirect information (from neighbor nodes).

Finally, the network information about the nodes has an expiration time, so after some time without contacts it is updated. The implementation of this mechanism is straightforward. When an event is received, it is marked with a time stamp, so in a given timeout an opposite event is generated.

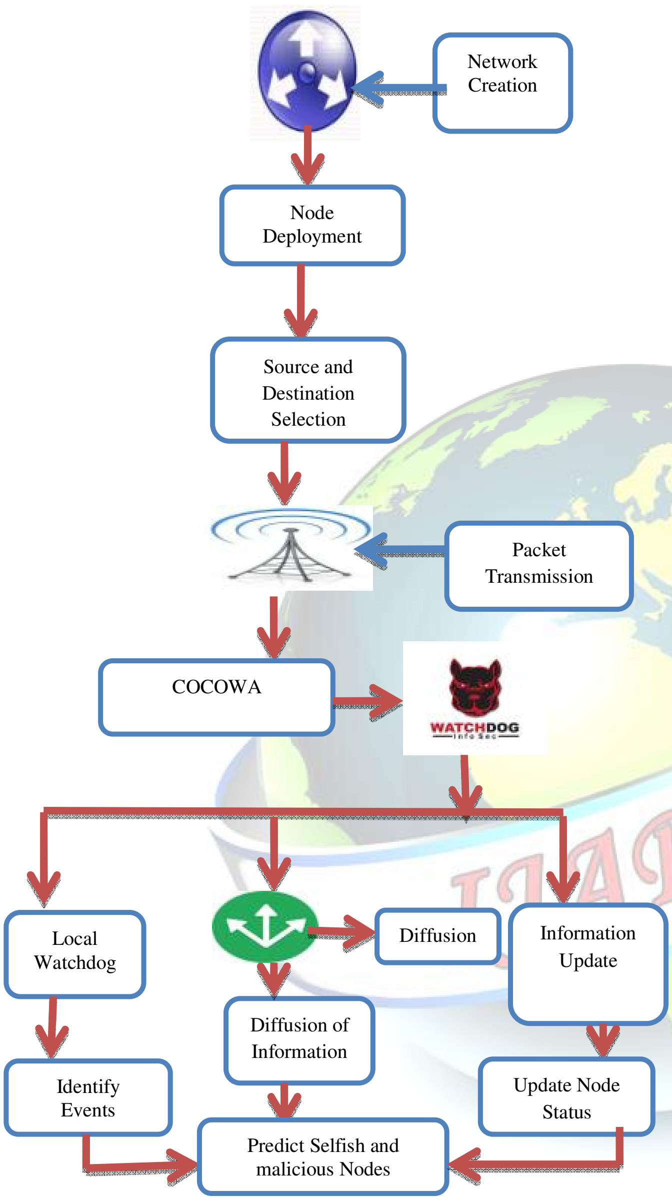

Fig. 1 System Architecture of CoCoWa

The advantages of this updating strategy are twofold. First, it can reduce the fast diffusion of false positive and false negatives. Nevertheless, this can produce a delay on the detection (more events are needed to get a better decision). Second, the decision about a selfish and malicious node is taken using the most recent information. For example, if a node had contact with the selfish node a long time ago (so it had a Positive state) and now receives several NegEvt in a row from other nodes, the state is updated to NEGATIVE.

IV. CONCLUSIONS

The co-operation on Mobile Ad-hoc networks is usually contact-based. Mobile nodes can directly communicate with each other if a contact occurs (that is, if they are within communication range). Supporting this cooperation is a cost intensive activity for mobile nodes. Nodes could have selfish behaviour, being unwilling to forward packets for others. Selfishness means that some nodes refuse to forward other nodes' packets to save their own resources. In the Existing System, when the watchdog detects a selfish node it is marked as a positive detection (or a negative detection, if it is detected as a non selfish node). Nevertheless, watchdogs can fail on this detection, generating false positives and false negatives that seriously degrade the behaviour of the system. For this Collaborative Contact based Watchdog (CoCoWa) have been introduced as a new scheme for detecting selfish and malicious nodes that combines local watchdog detections and the dissemination of this information on the network.

REFERENCES

[1] Bansal .S and Baker .M, “Observation-based cooperation enforce-ment in ad hoc networks” arXiv:cs.NI/0307012, 2003.

[2] Buchegger .S and Le Boudee .J-.Y, “Self-policing mobile ad hoc networks by reputation systems,” IEEE Commun. Mag., vol. 43, no. 7, pp. 101–107, Jul. 2005.

[3] Chaintreau .A, Hui .P, Crowcroft .J, Diot .C, Gass .R, and Scott .J, “Impact of human mobility on opportunistic forwarding algorithms,” IEEE Trans. Mobile Comput., vol. 6, no. 6, pp. 606–620, Jun 2007.

[5] Hortelano .J, Cano .J- .C, Calafate .C .T, de Leoni .M, Manzoni .P, and Mecella .M, “Black hole attacks in p2p mobile networks discovered through Bayesian filters,” in Proc. Int. Conf. Move Meaningful Internet Syst. , pp. 543–552, 2010.

[6] Hui .P, Crowcroft .J, and Yoneki .E, “Bubble rap: social-based forwarding in delay tolerant networks,” in Proc. 9th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. , pp. 241–250, 2008.