Adaptive CUSUM Algorithm to Detect Malicious Behaviors in Wireless Mesh Networks

Juliette Dromard, Rida Khatoun, Lyes Khoukhi

Adaptive CUSUM Algorithm to Detect Malicious behaviors in Wireless Mesh Networks

Juliette Dromard[1], Rida Khatoun[2], and Lyes Khoukhi[1]

[1] University of Technology of Troyes, 12 rue Marie Curie 10010 Troyes France
dromardj@utt.fr and lyes.khoukhi@utt.fr
[2] Telecom ParisTech 46 rue Barrault, 75013 Paris
rida.khatoun@telecom-paristech.fr

Abstract. Wireless mesh networks (WMNs) are very attractive networks as they are low cost and able to extend Internet rapidly in areas where other networks (e.g., Wi-Fi, MANETs, wired networks, 3G) cannot access due to their technical and/or economical limitations. However, these networks have to deal with security issues which prevent their deployment. In this paper, we propose a new reputation scheme which aims at preventing nodes from falsely detecting their neighbors as misbehaving due to packet loss over their links. The proposed reputation scheme is based on the fact that a link's packet loss ratio, when it is computed over a large quantity of observations, is quite stable over time. To detect misbehaving neighbors, a node, via its IDS, compares with the statistical method CUSUM (cumulative sum control chart) whether the distribution of packet loss rate observed for each of its neighbors follows the expected distribution or not. The validation of our solution shows that it allows to assign to nodes a trust value which reflects their real behavior.

Keywords: Wireless mesh networks, reputation computation, intrusion detection system

1 Introduction

Wireless mesh networks (WMNs) have very attractive characteristics, they are low cost, easy to install and maintain. WMNs allow to cover white zones and to extend Internet to last miles, to hostile areas and to areas where the installation of cables is not economically viable. They are made up of fixed nodes (i.e., mesh routers (MR)) which form the backbone of the network and relay the data of mesh clients (MC) from MR to MR till reaching a gateway which sends them to the Internet.

However, the deployment of WMNs is limited by several security issues; this is due essentially to the characteristics of a WMN (e.g., the wireless nature of the channel, the multi-hop ad-hoc routing, the location of the MRs in public areas, etc.) [1] [2] [3]. The wireless nature of the channel allows any attacker situated in a mesh router's coverage zone to listen to the transmission of every packet

that the MR forwards or sends. Furthermore, an attacker can easily scramble the data of the network by transmitting with a high power on the frequency used by the WMN. The attacker can also physically capture a MR as MRs are generally located in public areas, on a lamppost or on a bus stop [4] [2], for example. By capturing the routers, the attacker can retrieve the keys used for encryption, send false messages, drop packets, modify packets, and thus disrupts the network. The multi-hop nature of WMNs implies that every node may forward messages sent by other nodes. Thus, a WMN requires that every node collaborates in the routing process; hence, one compromised node can disrupt the whole network.

In order to overcome these security issues in WMNs, several security solutions based on cryptography schemes [5] [6] [7] have already been proposed. The amendment for mesh networking, the IEEE 802.11s, proposes also a security solution based on cryptography. Cryptographic schemes aim at preventing external nodes from entering the network as they don't possess the adequate cryptographic material to access the network. However, internal nodes can also misbehave and these solutions do not prevent such a situation. To detect internal misbehaving nodes in WMNs, researchers get interested in reputation schemes. In a reputation a scheme, every node monitors its neighbors via overhearing their transmissions, and, according to the outcomes of the monitoring, it assigns to each of them a reputation which is generally a value between 0 and 1 [8] [9] [10]. When the reputation value of a node is near to 0, the node is considered as misbehaving. In a reputation scheme, nodes generally monitor their neighbors by implementing the Watchdog IDS [11] [8] [10] [12]. The network interface card of a node which implements Watchdog is in promiscuous mode, thus, it can listen to every message sent in its covering zone even though it is not the destination of the message. A node can so check whether its neighbors correctly forward the message it sends to them or not, by overhearing their transmissions (see figure 1). In most reputation schemes based on Watchdog, a node assigns a reputation to each of its neighbors according to the number of packets it has correctly forwarded over the number of packets it has sent it. Then, a node interacts with a neighbor and forwards its packets according to its neighbor's reputation. The goal of reputation schemes is to isolate misbehaving nodes and/or to incite them to well-behave.

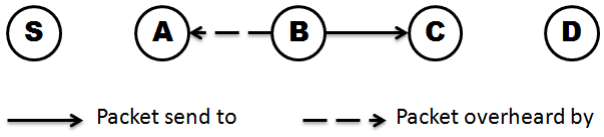

Fig. 1: Watchdog principle: Node A in a first step sends a packet to node B, B then, in a second step forwards this packet to node C. During this second step, node A overhears with the Watchdog IDS, whether node B forwards correctly to C the packet it has just sent to it.

However, a node's reputation can be distorted due to packet loss over the channel. Indeed, a node can consider that its neighbor has dropped its packet whereas the packet may, in fact, has been lost on the channel.
Furthermore, some experiments performed on real testbeds have shown that the packet loss rate on a WMN can be very high [13] [14] [15]. For example, the results of an experiment realized on a 38-urban wireless mesh network [15] have shown that most links pairs have intermediate delivery probabilities.

Thus, by not considering packet loss, Watchdog may launch many false positives, i.e., it may estimate that some nodes are misbehaving (i.e., drop packets), whereas in fact they are not (they just suffer from an important packet loss rate on their links). In consequence, reputation schemes which implement Watchdog may assign a bad reputation to a well-behaving node, due to packet loss over the channel. Thus, in these schemes a well-behaving node can be assigned a bad reputation and isolated unjustly from the network. In the rest of the paper, the term "bad node" refers to nodes which drops a certain percentage of packets and which can be either faulty, selfish or misbehaving whereas the term "good node" refers to node which does not drop any packet it receives.

In order to overcome this issue, we propose in this paper a new reputation scheme for WMNs:

- where every node integrates a reputation module made up of:
  - an IDS which aims at detecting bad nodes,
  - a computation reputation module which allows, based on the outcomes of the IDS, to assign a reputation to each node's neighbor .
- which has been validated with ns2 and the statistical R software [16]. The results of our validation shows that our system, contrary to most existing schemes, assigns to nodes a reputation which reflects their real behavior.

The rest of the paper is organized as follows. In the second section, we present a state of the art of the reputation systems in WMNs. Then, we introduce our packet loss rate model. Our IDS is proposed in the fourth section. In the fifth section, we present the computation reputation module of our solution. Then, we report the results of our evaluation, and finally, we conclude the paper.

2 Related works

In the following, we present related works in the field of reputation systems. Most of these works were developed for MANETs. However, as a mesh network can be considered as a MANET with fix mesh routers, all these solutions can be easily implemented in mesh networks.

Pathrater [17] is a reputation system based on Watchdog for MANETs (Mobile Ad-hoc networks) which aims at avoiding misbehaving nodes on path flows. Every node in Pathrater associates to each of its neighbors a rating which is adjusted according to Watchdog outcomes. To select a path, a node calculates the metric of every path to the destination by averaging the ratings of every node along the path and selects the path which possesses the highest metric.

Pathrater needs that every node has an opinion about every other node in the network which is only possible if nodes are very mobile.

In [9], Jaydip Sen proposes a reputation system based on Watchdog in MANETs. A node reputation is computed with first hand information (i.e., information gathered via direct exchanges) and weighted second hand information (i.e., information gathered via indirect exchanges) which are combined with the node's previous reputation. The simulations show the efficiency of this solution to reflect a node's behavior through its reputation. However, the authors don't specify any punishment mechanism to avoid misbehaving nodes.

In [11], Yu Li presents a reputation system for WMNs using a multi-path routing protocol which aims at enforcing nodes' collaboration. Each node computes its neighbors' reputation while considering first hand evidences collected via Watchdog, the node's delay and the position of the node on the path. When a node's reputation is under a certain threshold, an alert is broadcasted and the node is punished; its packets are not any longer forwarded. The simulations show that this reputation system stimulates nodes' cooperation. However, this solution is not protected against bad mouthing , i.e., against nodes which send false accusations.

In [18], the authors proposed a Reputation-Aware Multi-hop routing Protocol (RAMP) in MANETs which relies on the routing algorithm DSR (Dynamic Source Routing)[19]. RAMP is based on direct observations collected via Watchdog and on indirect observations. Indirect observations are collected by the source of a flow during the route maintenance. Indeed, each node on the route path must acknowledge every packet of data received from the source. If the source does not receive any acknowledgement from a node in a Round Trip Time (RTT), it decreases the node's reputation; otherwise, it increases it. The nodes' reputation is adjusted according to the AIMD (Additive-Increase-Multiplicative-Decrease) algorithm. The evaluation of RAMP shows that it could achieve 10-15% less packet loss than some existing reputation-based schemes. However, RAMP may lead to an important increase of overhead as every node on a flow path must send an acknowledgement to the source each time it receives a packet of data.

In [20], the authors proposed a reputation system which aims at detecting malicious nodes in MANET. The originality of this work lies in a multi-dimensional trust based outlier detection and a gossip-based outlier detection algorithm. They have proposed multiple metrics in order to detect outliers such as the PMR (packet modification rate), the PDR (packet drop rate) and the RTS (request-to-send) flooding rate. Indeed, according to the way a node misbehaves, the countermeasures to apply may be different. The gossip-based outlier detection algorithm aims at identifying the top k outliers (the value of k must be a priori known). However, the authors do not propose any scheme to isolate

misbehaving nodes and any method to fix the value of k.

[15] presents one of the major and most interesting studies of packet loss rate in a WMN. This article displays results obtained on an experimental 38-node urban 802.11b mesh network. They show that in WMNs, most pairs have intermediate delivery probabilities. Thus, packet loss must be considered in Watchdog in order to prevent nodes from wrong accusations.

As we can observe, many reputation systems are based on Watchdog and do not consider packet loss and CSMA/CA unfairness [20] [21] [18] [15] [11] [9] [17]; thus, they may suffer from false negatives. In order to avoid this issue, we propose in what follows a reputation computation system based on an IDS which consider packet loss.

3 Packet rate not overheard

In [15], the authors show that most links have intermediate loss rate. Furthermore, they point out that some links are bursty in terms of packet loss rate. However, they also show that "averaging over long time intervals (few seconds) smoothes out fluctuations" due to scattered burst; in other words, the packet loss rate, when computed over large intervals of times (few seconds), becomes quite stable over time. Thus, they display that "for most links, measuring a link loss rate over intervals as short as a few seconds is useful in predicting the near future. On the other hand, a small set of links (very bursty ones) varies substantially from one second to another". Furthermore, the authors in [22] have also shown via experiments on IEEE 802.11b wireless links that the packet loss rate on wireless links is quite stable. They assert that link qualities, at different times, are more or less similar and that the links'packet loss rate almost follow the same distribution, no matter the traffic is heavy or not. In order to prove this statement they performed the chi-square tests on observed data and found that the packet loss rates of links with the same length at different times follow the same distribution.
From the conclusions of these papers [22] [15], we model our network as a WMN where all links have a quite stable packet loss rate. Thus, the random variable which represents the packet loss rate of the directed link (i, j) denoted X_{ij}, is considered quite stable over time when it is computed over a quite large interval of time (few seconds) (see figure 2).

In the following, the percentage of packets that j forwards and i overhears among the set of packets sent by node i to node j is termed "packet rate not overheard by i from j". Let us consider three nodes, node i, j and k and four links between these nodes; links (i, j), (j, i), (k, j), (j, k) (see figure 3). To send a packet to node k, node i sends it to node j which forwards it to k. As node i monitors its neighbors, it can overhear j's communications. It can overhear successfully j forwarding its packet, if the packet is not lost over both (i, j) and (j, i), and is not dropped by j. Thus, the packet rate not overheard by i from j,

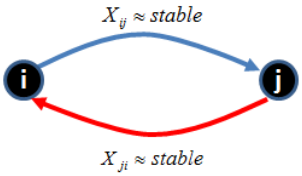

Fig. 2: Packet loss rate over links

denoted X^o_{ij}, depends, when node j is a good node, only on the packet loss rate of links (i, j) and (j, i). As the packet loss rate of these links is considered stable, the packet rate not overheard by i from node j can be also considered as stable (see figure 3). However, when j is a bad node, the packet rate not overheard depends also on the percentage of packets that node j drops. Thus, the distribution of packet rate not overheard by i from j is not the same depending on the node j 's behavior.

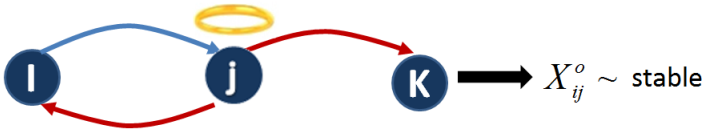

Fig. 3: Packet loss rate overheard from j by node i when j is a good node

4 Our intrusion detection system

Our detection intrusion system allows nodes to detect whether their neighbors drop packets or not; this is achieved by monitoring changes in the packet rate not overheard from each neighbor. Indeed, when a node misbehaves, it drops packets, which generates an increase in the rate of packets that it does not forward and so in the rate of packets that its neighbor does not overhear.

We assume that, every node i knows, for each of its neighbor j, the distribution of the packet rate, denoted X^o_{ij}, it does not overhear j forwarding when this latter is well-behaving and the standard deviation associated to this rate denoted σ^o_{ij}. The value of these parameters can be extracted by performing tests on the WMN's links before its deployment.

To detect changes in the packet rate not overheard, we have chosen the cumulative sum control charts (CUSUM) [23]. CUSUM is a sequential analysis technique which is used for monitoring detection changes. CUSUM detects changes in the distribution by periodically computing two sums, the upper control limit denoted C^+_z and the lower control limit C^-_z which are the cumulative deviation between the expected value and the observed value when the observed value is

respectively upper and lower than the expected one. When the upper control limit or the lower control limit exceeds a certain threshold, CUSUM launches an alert. CUSUM, in contrary to other methods of detection of change like the Shewhart control charts, enables to detect small shifts [24].

Our IDS aims at detecting an increase in the mean of the random variable, which means an increase in the packet rate not overheard. In our solution, each time, a node i sends m packets to a neighbour j, it monitors the number of packets denoted n it does not overhear j forwarding and can then compute a realization x_z of the random variable X_{ij}^o (representing the packet rate not overheard by i from j) as follows :

$$x_z = \frac{n}{m}$$

Indeed, m must be large enough so that, this rate is computed on an interval of time superior to a few seconds. When the IDS of a node i gets a new realization x_z, it then computes the upper control limit C_z^+:

$$C_z^+ = max[0, x_z - (X_{ij}^o + K) + C_{i-1}^+] \quad and\, C_0^+ = 1 \tag{1}$$

z represents the number of realizations, (i.e., the number of times it has already updated the upper control limit C_z^+), and K represents the reference value. More details about these parameters are given thereafter. Once, the IDS has updated the upper control limit, it checks whether it exceeds or not the decision interval H, i.e., if $C_z^+ \geqslant H$. If it does, the packet loss rate is assumed to have changed and node j is considered as misbehaving. To perform CUSUM, the values of the following parameters must be fixed:

• δ: it is the shift that the IDS wants to detect. This shift is expressed as a quantity of σ_{ij}^o. From this shift the out of control value of the packet rate not overheard is computed as follows: $X_t = X_{ij}^o \pm \sigma_{ij}^o \delta$

• K: it is the reference value. It is often chosen about halfway between the target value X_{ij}^o and the out of-control value X_t, in order to get good Average Run Length (ARL). The ARL is a measure of the performance of CUSUM.

• H: it is the decision interval. When the upper control limit or the lower control limit is above the decision interval H, we then consider that the process is out of control. It must be chosen so that we get a good ARL. There exists tables which allows, from the value of the parameter K, to choose the correspondent H in order to get a good ARL.

Thus, each time a node i gets a new realization x_z, it computes the upper control limit C_z^+ and checks whether this latter is above or not the decision interval H. If it is the case, then it assumes that the packet rate not overheard has changed and that j is misbehaving.

5 The reputation computation

Every node i stores about each of its neighbor j a reputation denoted R_{ij}. Once, a node i has performed CUSUM, it gets a value a_{ij} which is equal to 0

if CUSUM has launched an alert and 1 otherwise, and re-computes the value of R_{ij}. A new reputation R_{ij} is computed via the exponential moving average in order to consider older interactions:

$$R_{ij} = \beta R_{ij}^{old} + (1 - \beta)a_{ij} \quad (2)$$

with R_{ij}^{old} the latest reputation which was computed and β the forgetting factor which value is situated between 0 and 1. The choice of the value of β depends on the network. The exponential moving average allows to get a smooth forgetting of node's old actions; the weighting for each older reputation decreases exponentially and never reaches zero. Thus, the value of a node's reputation is between 1 and 0; closer its reputation is to 1, the better the node's reputation is.

The reputation R_{ij} that a node i gets about a node j at the bootstrap, is set by the network administrator. It depends on the trust that the network administrator has then on the nodes. For example, if all these nodes have been established by a same company, then the administrator can have at the bootstrapping an entire confidence in the WMN's nodes and give then the maximum reputation; 1.
Every node only needs to store, for each of its neighbors, its current reputation and the last value of its upper control limit C_z^+. Thus, if a node has n neighbors, then it has only $2n$ values to store; the complexity storage of our solution is very low. Furthermore, each node re-evaluates its neighbors' reputation after a few seconds. To compute a node's reputation, the upper control limit must be re-evaluated (see equation 1), this latter must then be compared to the decision interval H and finally the node's reputation is obtained with formula 2. Thus, if a node has n neighbors, then it has only $3n$ operations to perform in a few seconds. Furthermore, as every node computes its neighbors' reputation with only local data, our solution does not trigger any overload and is scalable.

6 Evaluation of our intrusion detection system

The aim of this evaluation is to show that by considering packet loss over links, our solution assigns to nodes a reputation which represents more precisely their real behaviour. We compare our solution with the reputation system proposed in [9] via the event discrete network simulator ns2. In [9], the authors propose a reputation system based on Watchdog where each node assigns to its neighbour a reputation which considers the historical of its interactions and the percentage of packets that it overhears its neighbour forwarding. We have chosen to compare our approach with [9] as it is quite a generic solution of reputation system based on Watchdog.

Our solution has been evaluated with two different WMN's topologies; a mesh topology and a cross topology (see figures 4 and 5). They both possess one gateway which is represented by a red node on the figures. We introduce in each topology a bad node which drops a certain percentage p of packets of data it receives with success. The parameters of the simulation are presented

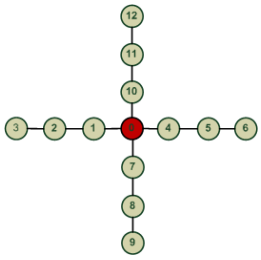

Fig. 4: Cross topology

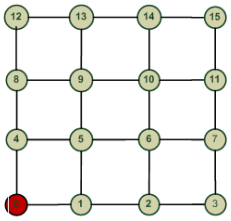

Fig. 5: Mesh topology

in the table 6. In the following, we assume that the network's links have been chosen so that the packet loss rate is not inferior to 0.5 and do not belong to the few set of links which are very burst so that the packet loss rate is quite stable. Our solution can deal with packet loss rates over links superior to 0.5, however, a mesh network with very bad links would not be very efficient. In such a case, only few packets would reach their destinations, so that we have decided to limit this rate to 0.5. However, our solution cannot deal with very bursty links as bursty links are most of the time quite unstable, so that we have chosen in our simulations to consider only links which are not very bursty. The packet loss rate of each link and the standard deviation associated to this rate are chosen according to a uniform normal law of parameters 0 and 0.5. Turning off links which burst is too important is indeed feasible as all the routers are, in WMNs, usually set up by a same entity. Thus, this entity can choose to turn off or on some links. According to [15], there is few very bursty links in WMNS, thus, turning off these links should not penalize much the WMN.

In the following, in order not to overload the figures, we have only represented the reputation of four nodes over times; three good nodes (node 1, 10 and 4) and one bade node (node 7).

Level	**Parameter**	**Value**
Signal propagation	Two-ray-ground model	
Packet loss rate	Mean of the rate	continuous uniform distribution of parameters 0 and 0.5
	Sandard deviation of the rate	continuous uniform distribution of parameters 0 and 0.5
Physical	Rate	54Mbit/s
	Frequency	$2,4GHz$
	PLCP preambule and header 's length	$20\mu s$
MAC	CSMA/CA	

Fig. 6: Values of the parameters used in our simulations

Figures 7 and 8 show the reputation of some mesh nodes in the WMN over time in the cross topology when the bad node drops 100% of the packets it receives with, respectively, the reputation system of [9] and ours. From these figures, we can notice that in existing solutions the reputation of good nodes depends on the value of the packet loss rate over their links and are not as high as they should be. Whereas in our solution good nodes possess the maximum trust which value is one. Both solutions give to the bad node a low trust which decreases quickly till 0. However, our solution takes longer to assign to the bad node a trust of 0 as it has to collect information during a few seconds about the node before assigning it a new trust value.

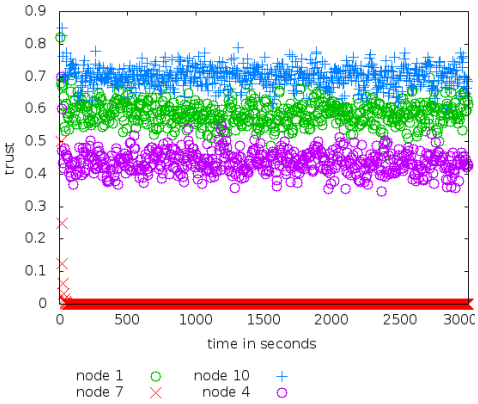

Fig. 7: The reference solution when $p = 100\%$

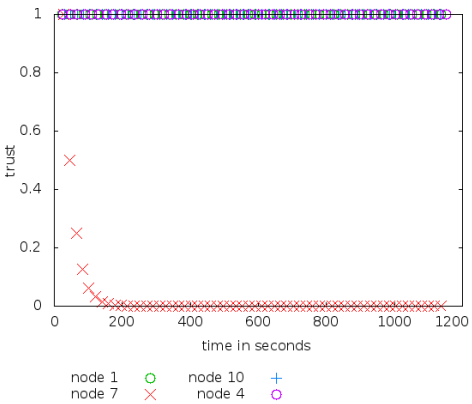

Fig. 8: Our solution when $p = 100\%$

Figures 9 and 10 show the reputation of some mesh nodes in the WMN over time in the cross topology, when the bad node drops 50 percent of the packets it receives with, respectively, the reputation system of [9] and our solution. From these figures, we can notice that with the reference solution, the reputation of good nodes depends on the value of the packet loss rate over their links. Whereas in our solution, good nodes possess the maximum trust. Both solutions give to the bad node a reputation with a low value. Our solution assigns to the bad node a lower reputation, however it takes quite a long time 200 seconds before the trust of node 7 decreases till the value 0. In the reference reputation system, we can notice that even though the reputation of the bad node is low, it is not very different from node 4 which packet loss rate over its links is important. Thus, our system allows to clearly identify the bad node whereas the reference solution cannot.

Figures 11 and 12 show the trust of some mesh nodes in the cross topology, when the bad node drops 20 percent of the packets it receives with, respectively, the reputation system of [9] and our solution. Our solution assigns to the bad node a low reputation; however, it takes quite a long time 500 seconds before the

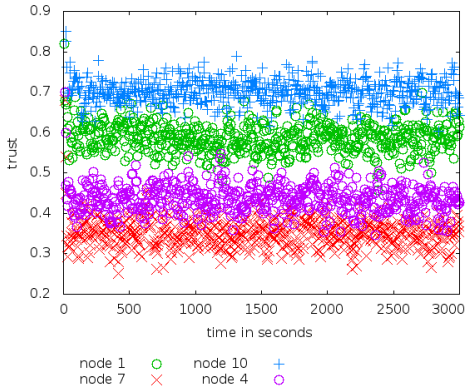

Fig. 9: The reference solution when $p = 50\%$

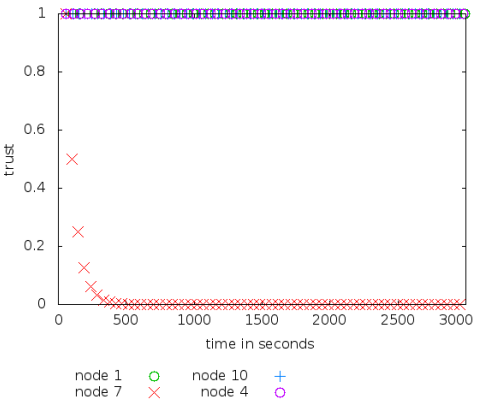

Fig. 10: Our solution when $p = 50\%$

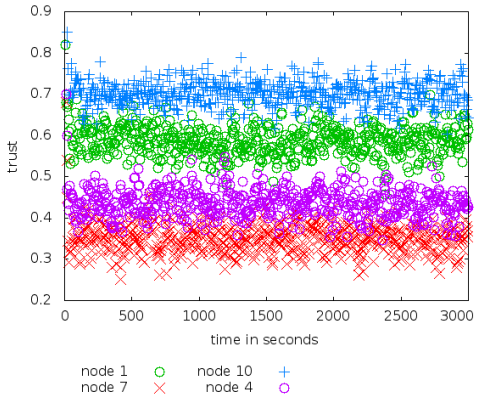

Fig. 11: The reference solution when $p = 20$ %

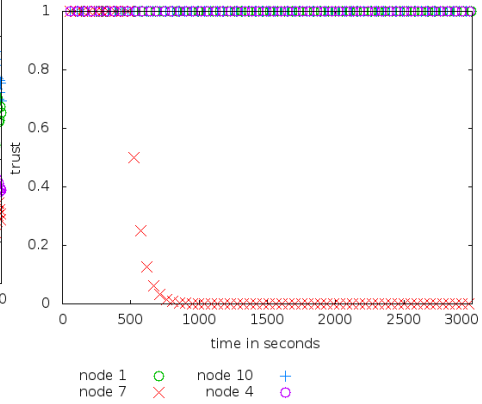

Fig. 12: Our solution when $p = 20$ %

trust of node 7 reaches 0. With the reference reputation system, we can notice that the reputation of the bad node is quite high and even higher than some good nodes' reputation (node 4 and 1). Thus, when a bad node drops a little percentage of packets of data, the reference reputation system cannot identify it, whereas our solution is still able to; however, it takes quite a long time.

7 Conclusion

In this article, we have proposed a new reputation system which considers packet loss rate in order to assign to nodes a reputation which reflects their behavior. Based on the fact that the packet loss rate over a link is quite stable over time, our solution allows to detect Greenhole and Blackhole by comparing the expected packet rate not overheard from a node with the observed one. If they differ, the

node is assigned a bad reputation. To detect changes in the packet rate not overheard from a node, our solution applies the statistical method CUSUM. We have shown that our solution has a low resource and computational complexity, generates no overhead and is scalable. We have validated our solution via ns2 and compared it to an existing solution. The results have shown that our solution detects efficiently bad nodes even when they drop few packets.

References

1. Akyildiz, I.F., Wang, X., Wang, W.: Wireless mesh networks: a survey. Comput. Netw. ISDN Syst. (2005) 445–487
2. Yi, P., Tong, T., Liu, N., Wu, Y., Ma, J.: Security in wireless mesh networks: Challenges and solutions. In: Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on. (2009) 423–428
3. Djahel, S., Begriche, Y., Nait-Abdesselam, F.: A bayesian statistical model to alleviate greediness in wireless mesh networks. In: Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. (2010) 1–6
4. Salem, N.B., Hubaux, J.P.: Securing wireless mesh networks. IEEE Wireless Communications (2006) 50–55
5. Hu, Y.C., Perrig, A., Johnson, D.B.: Ariadne: a secure on-demand routing protocol for ad hoc networks. Wirel. Netw. 21–38
6. : Ieee standard for information technology-specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 10: Mesh networking. IEEE Std 802.11s-2011 (2011)
7. Wang, J., Jiang, N., Li, H., Niu, X., Yang, Y.: A simple authentication and key distribution protocol in wireless mobile networks. In: Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on. (2007) 2282–2285
8. Yu, H., Shen, Z., Miao, C., Leung, C., Niyato, D.: A survey of trust and reputation management systems in wireless communications. Proceedings of the IEEE (oct. 2010)
9. Sen, J.: A distributed trust and reputation framework for mobile ad hoc networks. CoRR (2010)
10. Safaei, Z., Sabaei, M., Torgheh, F.: An efficient reputation-based mechanism to enforce cooperation in manets. In: Proceedings of the 4th international conference on Communications and information technology. (2010)
11. Li, Y.: A reputation system for wireless mesh network using multi-path routing protocol. In Zhong, S., Dou, D., Wang, Y., eds.: IPCCC, IEEE (2011)
12. Dromard, J., Khatoun, R., Khoukhi, L.: A watchdog extension scheme considering packet loss for a reputation system in wireless mesh network. In: Telecommunications (ICT), 2013 20th International Conference on. (May 2013) 1–5
13. Reis, C., Mahajan, R., Rodrig, M., Wetherall, D., Zahorjan, J.: Measurement-based models of delivery and interference in static wireless networks. In: Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. SIGCOMM '06, New York, NY, USA, ACM (2006)
14. Maheshwari, R., Jain, S., Das, S.R.: A measurement study of interference modeling and scheduling in low-power wireless networks. In: Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems. SenSys '08, New York, NY, USA, ACM (2008) 141–154

15. Aguayo, D., Bicket, J., Biswas, S., Judd, G., Morris, R.: Link-level measurements from an 802.11b mesh network. In: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications, New York, NY, USA, ACM (2004) 121–132
16. R Core Team: R: A Language and Environment for Statistical Computing. R Foundation for Statistical Computing, Vienna, Austria. (2013)
17. Marti, S., Giuli, T.J., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th annual international conference on Mobile computing and networking. (2000)
18. Tan, H.: Ramp: a reputation-aware multi-hop routing protocol in wireless ad-hoc networks. In: Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, New York, NY, USA, ACM (2011)
19. Johnson, D.B., Maltz, D.A.: Dynamic source routing in ad hoc wireless networks. In: Mobile Computing, Kluwer Academic Publishers (1996) 153–181
20. Li, W., Parker, J., Joshi, A.: Security through collaboration and trust in manets. Mobile Networks and Applications (2012) 342–352
21. Zaidi, Z., Landfeldt, B.: Monitoring assisted robust routing in wireless mesh networks. Mobile Networks and Applications (2008) 54–66
22. Jiang, H., Chen, S., Yang, Y., Jie, Z., Leung, H., Xu, J., Wang, L.: Estimation of packet loss rate at wireless link of vanet–rple. In: Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on. (Sept 2010) 1–5
23. Basseville, M., Nikiforov, I.V.: Detection of abrupt changes: theory and application. Prentice-Hall, Inc., Upper Saddle River, NJ, USA (1993)
24. Montgomery, D.: Introduction to Statistical Quality Control. third ed. John Wiley&Sons (1996)