Watchdog Intrusion Detection Systems: Are They Feasible in MANETs?

Jorge Hortelano, Juan-Carlos Cano, Carlos T. Calafate and Pietro Manzoni

Departamento de Informática de Sistemas y Computadores

Universidad Politécnia de Valencia

Camino de Vera, S/N - 46022 Valencia, Spain

jorhorot@upvnet.upv.es; {jucano, calafate, pmanzoni}@disca.upv.es

Abstract

Watchdogs are the basis of different Intrusion Detection Systems. They have the advantage of using only local information and therefore, they are robust to most of the attacks. Although importance of this mechanism is clear, it is hard to find studies that seriously test the watchdog in wireless mobile scenarios with high degrees of mobility, a characteristic of any Mobile Ad Hoc Network (MANET). In this work we demonstrate that an extra effort must be done to solve some watchdog drawbacks that are still present when using them in MANET scenarios.

1 Introduction

The widespread adoption of wireless technologies has caused the computer networks concept to be re-shaped. As a consequence, new kinds of networking architectures have been developed in the last years to cope with some scenarios where the traditional wired networks are not a possible solution. Mobile ad hoc networks (MANETs) [1] are a clear example of a new novel communications paradigm based on wireless technology and designed specifically to be used in scenarios where a fixed infrastructure is impossible to deploy. This network architecture mainly differs from other conventional wireless networks by having no fixed infrastructure. A MANET consists of mobile nodes interconnected by multihop communication paths where nodes themselves define the topology. Therefore, the topology of the network changes dynamically as mobile nodes join or depart from the network, or when radio links between nodes become unusable. These changes on the topology are managed by specific protocols such as AODV [2], OLSR [3] or DYMO [4], which spread the information about network changes among all nodes of the MANET.

The upgrowth of MANETs becomes evident if we think about the specific target scenarios. Special situations without any previous infrastructure, like emergency missions, military operations or ad hoc meetings rely on this network architecture to deploy a communications system. However, the absence of infrastructure makes MANETs more vulnerable to attacks than other conventional networks. Since the protocols designed for MANETs are based on the cooperation among nodes (and, therefore, on the confidence on these nodes), its specifications cope well with network topology changes. However, it also makes them vulnerable against malicious attacks.

There are several kinds of attacks that can take place in MANETs, but in this work we will only focus solely on the attacks that are specific to the data transmission process. One of the main attacks against ad hoc networks affecting their routing protocols are named routing-disruption attacks. Such attacks can be considered as instances of a denial-of-service (DoS) attack, since they compromise the routing of packets, thus affecting the availability of certain (or all) network and applica-

tion services. An example of these kinds of attacks is the selfish node, which uses the network but does not cooperate, saving battery life for its own communications. Another similar attack is the blackhole, which intends to disrupt the communication with its neighbourhood by attracting all traffic flows in the network and then dropping all packets received without forwarding them to their final destination.

The existence of these attacks makes the network availability quite unpredictable. Notice that network availability is a minimum requirement for developing any commercial system, and MANETs are not an exception. Therefore, and extra effort must be done to achieve an acceptable security degree. In particular, trustworthiness is essential for the practical exploitation of these networks.

Several techniques have been developed to avoid these kinds of attacks. Existing ad hoc security solutions can be classified into three main categories [5]: key management, secure routing, and cooperation enforcement. Key management guarantees the identification and copes with all the problems concerning keys; secure routing uses the established keys to ensure the authentication, the confidentiality and the integrity in both the topology discovery and the data forwarding phases; finally, cooperation enforcement fights selfish behaviors and encourages the cooperation between nodes.

In the scope of this work, we will focus on the last category. In this context, intrusion detection systems (IDS) aim at monitoring the activity of the nodes in the network in order to detect misbehavior. A basic module in the construction of such systems is the watchdog [6], a component used for the detection of selfish nodes and malicious attackers. When a node forwards a packet, the watchdog verifies that the next node in the path also forwards the packet. Other reputation systems, like the Pathrater [7] and Routeguard [8] solutions, isolate and/or punish misbehaving nodes or routes by decreasing their trustability rates.

In this work, we test an implementation of a watchdog module using the ns2 simulator [9]. Although watchdogs seem to be a useful tool for IDS, and also the base for other related techniques, our results show that they are highly affected by node mobility, an intrinsic characteristic of MANETs. This affects the credibility of the watchdog when applied to MANETs: the higher the mobility is, the more false positives and false negatives the watchdog incurs in. Hence, in this work we make a deep study of the watchdog and its problems. Based on the obtained result we propose to use a bayesian filtering technique to filter the noise caused by node mobility in the watchdog monitoring process.

The rest of this paper is organized as follows. Section 2 presents the related work based on the watchdog. Section 3 presents our evaluation of this methodology and its problems. In Section 4 we discuss more deeply how mobility affects the standard watchdog. Section 5 discusses our proposal for improving the watchdog and attenuate the false positive and false negative problems. Finally, Section 6 concludes this work.

2 Related work

The watchdog [6] method allows detecting misbehaving nodes. When a node forwards a packet, the watchdog set in the node ensures that the next node in the path also forwards the packet. The watchdog does this by listening to all nodes within transmission range promiscuously. If the next node does not forward the packet then it is tagged as misbehaved. A match confirms that the packet has been successfully forwarded, causing the neighbour's trustworthiness to be increased. If a packet is not forwarded within a timeout period, then a failure tally for the node responsible for forwarding the packet is incremented. If this tally exceeds a predetermined threshold, then the node is termed as malicious.

Due to the effectiveness of the watchdog and its relative easy implementation, several proposals use it as the basis of their IDS solutions. Therefore, we can find in the literature several approaches that are watchdog-based. In the Pathrater approach [7], each node uses

the information provided by watchdogs to rate neighbors. The Routeguard mechanism [8] combines the watchdog and Pathrater solutions to classify each neighbor node as Fresh, Member, Unstable, Suspect or Malicious. As can be seen, watchdogs are at the core of the most important types of IDS solutions for ad hoc networks. The main advantage of the watchdog is to offer a node the possibility of detecting an attacker only using local information, thus avoiding that a malicious node affects the decisions made by the mechanism. In contrast, the watchdog has a well known vulnerability: it is vulnerable to the attack of two consecutive malicious nodes, where the watchdog can only monitor the first one while the second malicious node performs an attack. Some previous works [10, 11] define techniques for avoiding the problem of cooperative blackholing in MANETs, but they also have some limitations. For example all of the described methodologies are based on the AODV protocol and require a change in the implementation of AODV. Thus, we would need to implement a specific IDS for each routing protocol used. In Section 5.2 we proposed a protocol independent solution to counter this problem.

3 Watchdog evaluation

We perform several tests using the ns-2 [9] simulator. In order to do this, we implemented a specific watchdog module for this simulator (available at `http://safewireless.sourceforge.net/`). Using this simulator allows us to test networks with a large number of nodes, changing the number of attackers and the mobility of them. Figure 1 shows a preliminary study of how the percentage of malicious nodes and the total number of nodes of the scenario affects the probability that an attack is performed in a traffic flow. As we can see, not only the percentage of attackers affects the probability of found an attack in one test, also the number of total nodes of the scenario affects it.

Afterwards we implemented the watchdog mechanism for this simulator and performed several tests varying the mobility of the nodes

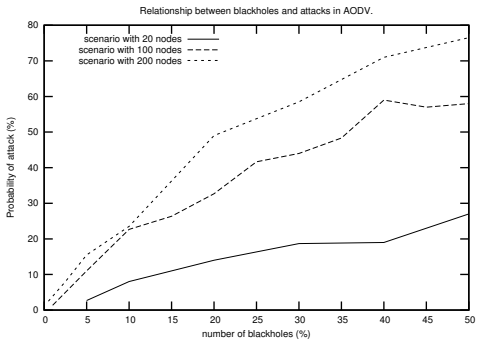

Figure 1: Probability of an attack when varying the number of nodes and the percentage of attackers.

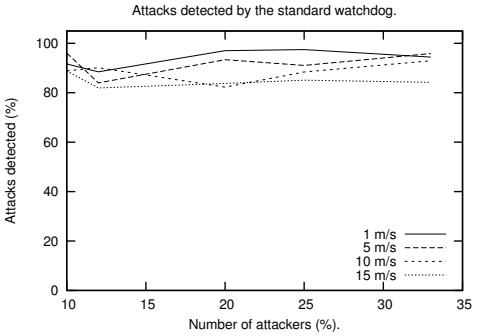

Figure 2: Attacks detected by the watchdog when changing the mobility of a scenario.

and the number of attacks to assess the effectiveness of the watchdog. Figure 2 shows the results obtained with different parameters. We can see that mobility clearly affects the number of attacks detected. It decreases when mobility is increased. With a mobility of 1 m/s, near by 100% of the attacks are detected, but, when we increase mobility to 15 m/s, the detection is reduced to 80%. These results are independent of the number of malicious nodes deployed in the simulation. It affects the total number of attacks, but not the ratio of the attacks detected.

Another studied effect is the false positives problem. Figure 3 presents a ratio between false positives and attacks in the simulation.

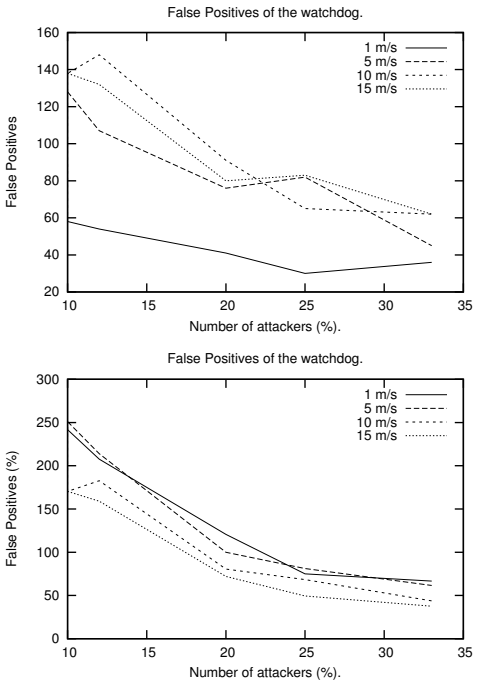

Figure 3: Number of false positives generated (up) and false positive ratio (bottom) when changing the mobility of a scenario.

Here we can see that, when the degree of mobility and the number of nodes increase, the ratio of false positives decreases. Despite the fact the number of false positives is increased when we increase the mobility, the number of attacks is also increased, causing the number of attacks detected to be increased too. Therefore, the total ratio of false positives is decreased.

Overall, we conclude that the watchdog does not cope well with mobility, especially at high node speeds. In fact, the higher the node speed is, the more false positives and false negatives the watchdog incurs in. A deeper study about the relationship between watchdog performance and mobility is discussed in Section 4.

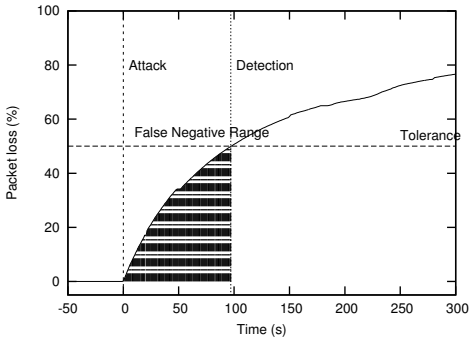

Figure 4: Time detection for the watchdog.

4 Detected drawbacks of the watchdog mechanism

Besides the well known problem of the collaborative attacks, the main problems detected for watchdog mechanisms are: (i) how the environmental noise affects the watchdog and the difficulties to cope with it, and (ii) how the watchdog can infer whether a node is in range or not when nodes has a high degree of mobility.

Although the watchdog methodology should be enough to detect malicious nodes, packet collisions and signal noise cause, in practice, the false positives and false negatives problem to emerge. It is difficult for a watchdog to differentiate whether the loss of a packet is due to an attack or a collision. In this latter case, if an alert is generated, it may lead to the generation of a false positive. This effect is palliated by the use of a tolerance threshold. This tolerance means that a node will ignore a percentage of packet loss. Hence the value of this parameter represents a trade-off between detection speed and false positives. If we pick a low tolerance value, the medium noise would cause benevolent nodes to be marked as malicious. If the tolerance value is set to high, the watchdog will need too much time to detect an attack. In fact, when it is performed in MANETs with a high degree of mobility, the possibility of detecting an attack becomes minimal.

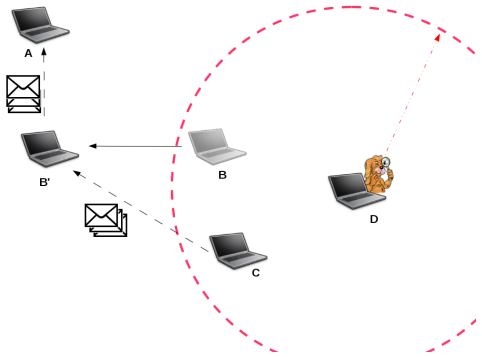

Figure 5: False positives due to watchdogs timeouts.

Figure 4 shows a schema of the watchdog response in the presence of an attack. In this experiment there is an interval of almost 90 seconds where an attack can be performed unnoticed by the watchdog. As shown in this figure, the watchdog methodology requires sniffing enough data packets to decide whether a node is an attacker. This means that more time is needed to make a decision compared to a network without a tolerance threshold. If the attacker is moving, there is a possibility that the malicious node moves outside the watchdog signal range, and thus it would not be detected. Therefore, false negatives can appear, and both intermittent and temporal attacks may remain undetected.

The second problem is how a watchdog can determine whether a neighbour is in range or not. As we remarked before, the watchdog has the advantage of using only local information, but this has also some disadvantages, such as the watchdog does not knows when a neighbour goes out of range. This problem is solved by using timeouts: when the time that passes after the last neighbour packet listened surpasses a certain value, the watchdog considers this neighbour to be out of range and will not considers it for future tests. The main problem of this strategy is how to find the best timeout. A low value forces the watchdog to restart all calculations for a neighbour before a decision about it being malicious or not is made, possibly not detecting a malicious node, thus causing false negatives. A high value causes that, when a neighbour goes out of range, the watchdog would consider it to be in range for a long time. In that case, the watchdog would expect retransmissions from this neighbour, but would not listen to any. As a consequence, it would decide that this neighbour is a malicious node, thus causing false positives. Figure 5 shows an example of a false positive caused by a high timeout value. When node B moves to position B', the watchdog of node D thinks that B is within range until the timeout is triggered. As a consequence, D would expect to listen to the packets forwarded by B, and otherwise, it would mark it as being a malicious. This is the main reason why, in Section 3, the false positives are slightly increased when we increase the mobility of the nodes. We can also consider this as another type of scenario affecting the watchdog performance.

Next we propose a strategy to improve the watchdog and mitigate the false positives and false negatives problem.

5 Solutions proposed

We propose a technique similar to the one used in SPAM filters used for emails: bayesian filters. Additionally, to avoid collaborative attacks, we propose an information exchange strategy similar to a voting system.

5.1 Bayesian filters

In the previous section we showed how mobility affects the capacity of the watchdog for detecting an attacker. In the literature we can find a reliable and extensive set of tools for detecting abnormal behaviours considered malicious in other fields, such as the SPAM filters. A SPAM filter can segregate illegitimate spam email from legitimate email. This email filters are normally based on bayesian filters [12], which allow the mail client to learn about the user decisions. Bayesian filters are not only useful for detecting SPAM. Other works such as [13, 14] also successfully use bayesian filters for predictions of abnormal be-

haviour. S. Buchegger et al. [13] use it for implementing reputation systems for P2P and MANETs, while M. de Leoni et al. [14] use bayesian filters for predicting disconnections on a MANET. Thus, Bayesian filters seem to be a useful tool for detecting abnormal behaviour and, therefore, a good tool for improving our intrusion detection system. Our proposal is to combine bayesian filters with the information obtained by a watchdog to design a tool capable of segregating malicious nodes from benign ones using historical information to prevent both false positives and false negatives.

5.2 Detecting collaborative attacks

A cooperative attack takes place when two or more nodes act together to perform an attack. This kind of attack is similar to the standard black-hole attack, but needs an extra node (*M1*) that will forward all packets to the node performing the black-hole (*M2*). The node that performs the attacks acts as a standard black-hole, and meanwhile the cooperative node keeps sending packets to it despite it being detected as malicious. The neighbour watchdog of *M1* detects *M1* as a non-malicious node because it is forwarding all the packets received. However, M1 does not mark M2 as being malicious because it is an accomplice. Hence, the attack can not be avoided by a classical watchdog.

Our proposal is not protocol-dependent: if we use a system for sharing information, as proposed on some papers [15, 16], we can use a voting system to decide if a node is malicious or not. Since all nodes have access to the votes of the other nodes, we can predict if a node k is performing an abnormal behaviour. A node k is doing an abnormal behaviour when it is forwarding packets to another node j that is previously marked as being malicious. Since all neighbours share the voting information, every node can determine whether the k's behaviour is correct, or mark it as a malicious node too.

6 Conclusions and future work

In this paper we make a deep study of the watchdog methodology evaluating its advantages and disadvantages. As the main advantage we can say that the watchdog only needs local information and, therefore, it becomes quite difficult for it to be badly influenced by another node. In contrast, it has two disadvantages (i) the watchdog is vulnerable to cooperative attacks and (ii) it is not so accurate when we increase nodes mobility. Hence, we must improve this mechanism if we want to use it in MANETs or even in other scenarios such as Vehicular Ad hoc Networks (VANETs). Moreover, if we consider that the watchdog is a basic module for several different IDS, doing an extra effort for improving it becomes a necessity.

We propose improvements that can cope well with the watchdog weaknesses based on bayesian filters. We consider that this technique can be adopted in the scope of our IDS with success. Another improvement to avoid the collaborative black-hole attack is proposed in this work. A secure exchange of information among nodes allows determining whether if a node is acting as a accomplice, and also marks it as being malicious.

As future work, we will deeply study both proposals, we will implement them for the ns-2 simulator, and we will perform an empirical test to validate they and confirm the improvements obtained.

7 Acknowledgments

This work was partially supported by the Ministerio de Educación y Ciencia, Spain, under Grant TIN2008-06441-C02-01, and by the "Ayudas complementarias para proyectos de I+D para grupos de calidad de la Generalitat Valenciana (ACOMP/2010/005)".

References

[1] M. Conti and S. Giordano. Multihop ad hoc networking: The theory. *Commu-*

nications Magazine, IEEE, 45(4):78–86, April 2007.

[2] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (AODV) routing. Request for Comments 3561, Network Working Group, http://www.ietf.org/rfc/rfc3561.txt, July 2003. Experimental.

[3] T. Clausen and P. Jacquet. Optimized link state routing protocol (olsr). Request for Comments 3626, MANET Working Group, http://www.ietf.org/rfc/rfc3626.txt, October 2003. Experimental.

[4] I. D. Chakeres and C. E. Perkins. Dynamic MANET on-demand (DYMO) routing protocol. *IETF Internet Draft*, November 2007.

[5] Xiaoyun Xue, Jean Leneutre, Lin Chen, and Jalel Ben-Othman. Swan: A secured watchdog for ad hoc networks. *IJCSNS International Journal of Computer Science and Network Security*, 6(6):209–219, June 2006.

[6] S. Marti, T.J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. 6th MobiCom, Boston, Massachusetts, August 2000.

[7] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 255–265, New York, NY, USA, 2000. ACM.

[8] Hasswa, A., Zulkernine, M., and Hassanein, H. Routeguard: an intrusion detection and response system for mobile ad hoc networks. In *Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob'2005)*, volume 3, pages 336–343. IEEE, August 2005.

[9] USC/ISI UC Berkeley, LBL and Xerox PARC researchers. Network Simulator - ns (Version 2). Available at: http://www.isi.edu/nsnam/ns/, 1998.

[10] Latha Tamilselvan and Dr. V Sankaranarayanan. Prevention of co-operative black hole attack in manet. In *Journal Of Networks (JNW)*, volume 3, pages 13–20, may 2008.

[11] H. Weerasinghe and Huirong Fu. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In *Future Generation Communication and Networking (FGCN 2007)*, volume 2, pages 362–367, Dec. 2007.

[12] M Sahami, S Dumais, D Heckerman, and E Horvitz. A bayesian approach to filtering junk e-mail. In *AAAI-98 Workshop on Learning for Text Categorization*, 1998.

[13] Sonja Buchegger and Jean-Yves Le Boudec. A robust reputation system for p2p and mobile ad-hoc networks. 2004.

[14] M. de Leoni, S. R. Humayoun, M. Mecella, and R. Russo. A bayesian approach for disconnection management in mobile ad-hoc network. In *Ubiquitous Computing and Communication Journal*, 2008.

[15] Lukasz Juszczyk, Harald Psaier, Atif Manzoor, and Schahram Dustdar. Adaptive query routing on distributed context - the cosine framework. In *International Workshop on the Role of Services, Ontologies, and Context in Mobile Environments (ROSOC-M)*. 10th International Conference on Mobile Data Management (MDM 09). IEEE, may 2009.

[16] Lukasz Juszczyk and Schahram Dustdar. A middleware for service-oriented communication in mobile disaster response environments. In *6th International Workshop on Middleware for Pervasive and Ad-Hoc Computing (MPAC)*. 9th Middleware Conference. ACM/IFIP/USENIX, december 2008.