An Improved Watchdog Intrusion Detection Systems In Manet

[1] *Tushar Sharma,*[2] *Mayank Tiwari,*[3]*Prateek kumar Sharma,* [4]*Manish Swaroop* [5]*Pankaj Sharma*

Information Technology Department, ABES Engineering College, Ghaziabad (U.P.), India

Affiliated to

Gautam Buddha

Abstract- There are various watchdog intrusion detection systems proposed to secure MANET. The watchdog IDS have advantage over other IDS is that they use only their 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 degree of mobility, a characterstics of any Mobile Adhoc Network.In this paper we demonstrate that an extra effort must be done to solve some watchdog drawbacks that are still present when using them in MANET's scenarios.

Keywords- kalman, watchdog , Bayesian ,MANET ,AODV.

1.INTRODUCTION

The widespread adoption of wireless technologies has caused the computer networks concept to be re-shaped. As a consequence, new kind of network architectures have been developed in the previous years to cope with some scenarios where the traditional wired networks are not a possible solution.

A MANET consists of mobile nodes interconnected by multi hop 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 [1], OLSR [2] or DYMO [3], which spread the information about network changes among all nodes of the MANET.

In a mobile ad hoc network, it is much more vulnerable to attack than a wired network due to its limited physical security, dynamically changing network topology, energy constrained operations and lack of centralized administration. 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 application.

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 black hole, which intends to disrupt the communication with its neighborhood by attracting all traffic flows in the network and then dropping all packets received without forwarding them to their final destination.

Watchdog mechanism proposed in [4] is a monitoring method used for ad hoc and sensor networks, and is the basis of many misbehavior detection algorithms and trust or reputation systems. The basic idea of the watchdog mechanism is that of nodes (called watchdogs) police their downstream neighbors locally using overheard messages in order to detect misbehavior. If a watchdog detects that a packet is not forwarded within a certain period or is forwarded but altered by its neighbor, it deems the neighbor as misbehaving. When the misbehavior rate for a node surpasses certain threshold, the source is notified and subsequent packets are forwarded along routes that exclude that node [4].

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 [5] and Routeguard [6] solutions, isolate and/or punish misbehaving nodes or routes by decreasing their trustability rates.

2. RELATED WORK

The watchdog [7] 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 [5], each node uses the information provided by watchdogs to rate neighbors. The Routeguard mechanism [6] 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 [8,9] 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.

The main challenge for most watchdog mechanisms is the unreliable wireless environment. Due to possible reasons such as channel fading, collision with other transmissions, or interference, even when the source node and the attacker are both within the communication range, the watchdog may not be able to overhear every transmission and therefore may be unable to determine whether there is an attack. To mitigate the misbehavior of the malicious nodes, a watchdog mechanism must achieve the following two goals:

(a) Malicious behavior in the network should be detected.

(b) The throughput under the detection mechanism should be comparable to the throughput without detection if there is no attack.

These two goals seem to have conflict in interest. On one hand, more redundancy is required to improve the probability of detection. On the other hand, higher throughput requires redundancy to be reduced.

A variant of watchdog mechanism is proposed in [10] where next-hop's behavior is measured with the local evaluation record, defined as a 2-tuple: packet ratio and byte ratio, forwarded by the next-hop neighbor. Local evaluation records are broadcast to all neighbors. The trust level of a node is the combination of its local observation and the broadcasted information. Trust level is inserted to the RREQ (Route Request). Route is selected in the similar way to AODV (Ad hoc On Demand Distance Vector) [11]. Although many ad hoc trust or reputation systems such as [12], [13] and adopt different trust level calculation mechanism, the basic processes are similar to [10], including monitoring, broadcasting local observation, combing the direct and indirect information into the final trust level. Recently, the security issue in network coding systems has drawn much attention. Due to the *mixing* nature of network coding, such systems are subject to a severe security threat, known as a *pollution attack*, where attackers inject corrupted packets into the network.

3. WATCHDOG ANALYSIS

We perform several tests using the ns-2 [14] simulator. In order to do this, we implemented several watchdog modules for this simulator (available at http://www.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 throughput of optimal AODV protocol.

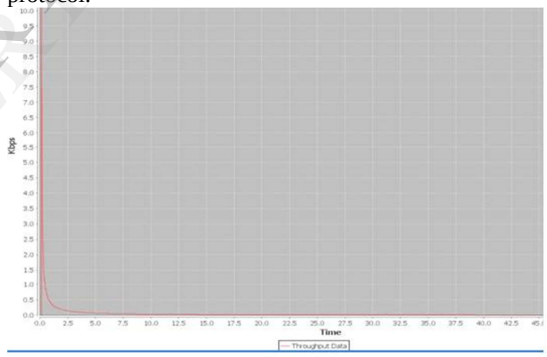

Figure1: Throughput of optimal AODV protocol

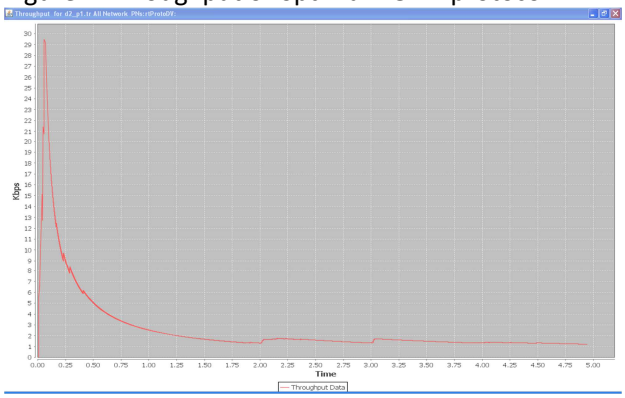

Figure2: Throughput of basic watchdog +AODV protocol

Figure 2 shows the throughput of basic Bayesian watchdog+ AODV protocol.
We implemented the watchdog mechanism for this simulator and performed several tests varying the mobility of the nodes and the number of attacks to assess the effectiveness of the watchdog. We check the false positive problem.

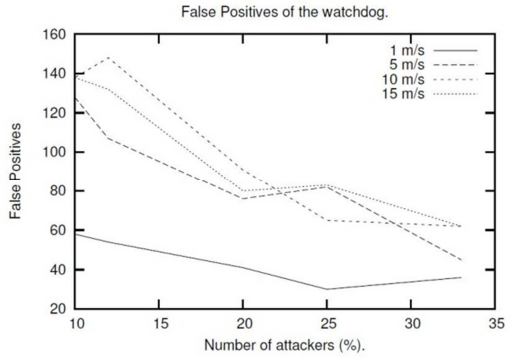

Figure4.1: Ratio between false positives and attacks in the basic Bayesian watchdog simulation

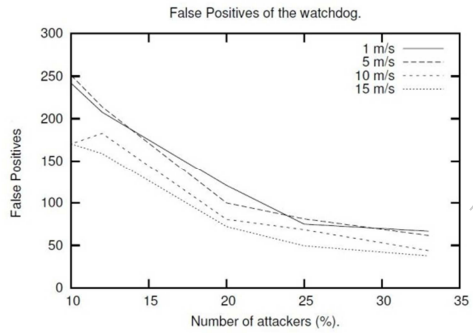

Figure 4.2: Ratio between false positive and attacks in the kalman filter watchdog simulation

Figure 4.1 and 4.2 the presents a ratio between false positives and attacks in the simulation.
In AODV we cannot find the false positive so ratio between false positive and attacks cannot be possible to identify. To overcome this problem we used watchdog technique with AODV to improve the security of MANET.
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.

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 till now Detected drawbacks of the watch-dog mechanism Besides the well-known problem of the collaborative attacks, the main problems detected for basic Bayesian 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-of 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.

4. SOLUTIONS PROPOSED

We propose a technique similar to the one used in SPAM filters used for emails: kalman filters which is better than optimized Bayesian filter additionally, to avoid collaborative attacks, we propose an information exchange strategy similar to a voting system.
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 behaviors 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 basic Bayesian filters [15], which allow the mail client to learn about the user decisions. Basic Bayesian filters are not only useful for detecting SPAM. Other works such as [16, 17] also successfully use Bayesian filters for predictions of abnormal behavior. S. Buchegger et al. [16] use it for implementing reputation systems for P2P and MANETs, while M. de Leoni et al. [17] use
Basic Bayesian filters for predicting disconnections on a MANET. Basic Bayesian filters seem to be a useful tool for detecting abnormal behavior but they have some disadvantages. Therefore, kalman filter is a good tool for improving our intrusion detection system. So our proposal is to use kalman filters and combined it with the information obtained by a watchdog to design a tool capable of segregating malicious nodes. Because kalian filter gives better results than basic Bayesian filter.

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 neighbor 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 cannot be avoided by a basic watchdog. Our proposal is not protocol-dependent: if we use a system for sharing information, 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 behavior. A node k is doing an abnormal behavior when it is forwarding packets to another node j that is previously marked as being malicious. Since all neighbors share the voting information, every node can determine whether the k's behavior is correct, or mark it as a malicious node too.

5. CONCLUSION 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 kalman 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 an accomplice, and also marks it as being malicious.

6. References

[1].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.

[2].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.

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

[4]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *MobiCom ’00: Proceedings of the 6th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2000, pp. 255–265.

[5]. 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.

[6] 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.

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

[8]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.

[9] 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.

[10]T. Ghosh, N. Pissinou, and K. Makki, “Towards designing a trusted routing solution in mobile ad hoc networks,” *Mob. Netw. Appl.*, vol. 10, no. 6, pp. 985–995, 2005.

[11] C. Perkins and E. Royer, “Ad-hoc on-demand distance vector routing,” *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA ’99. Second IEEE Workshop on*, pp. 90–100, Feb 1999.

[12] S. Buchegger and J.-Y. Le Boudec, “Performance analysis of the confidant protocol,” in *MobiHoc ’02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*.New York, NY, USA: ACM, 2002, pp. 226–236.

[13] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, “A quantitative trust establishment framework for reliable data packet delivery in manets,” in *SASN ’05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*. New York, NY, USA: ACM, 2005, pp. 1–10.

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

[15]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.

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

[17] 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.