ISSN:0975-9646

Prevention Of Black Hole Attack Using Improvised Watch Dog Through Data Accumulation

K. R. Viswa Jhananie [1] , Dr. C. Chandrasekar [2]

[1]*Department of Computer Science,Sheshadripuram Academy of Business Studies, Bangalore, Karnataka, India.*
[2]*Department of computer science,Periyar University, Salem, Tamil Nadu, India.*

Abstract **- A mobile Ad-hoc network (MANET) is an autonomous collection of mobile devices. They co-operate in a distributed manner to provide necessary network functionality. Since MANETs are easy to deploy , they are useful in natural disasters, where the network can immediately be constructed. But, since the nodes are mobile in nature, MANETs are vulnerable to many attacks. Black hole attack is one of the serious attack in MANETs. In this paper, we discuss about black hole attack and provide a security measure using monitoring technique called watchdog.**

Keywords **- Black hole attack, malicious node, MANET, secured data, watch dog.**

I. INTRODUCTION

In MANET, during normal operation, the inter node connectivity may change frequently. The nodes are free to move randomly and they organize themselves arbitrarily. MANETs follow dynamic topology where nodes may join and leave the network at any time and the multi-hop routing may keep changing as nodes join and depart from the network[1]. The nature of MANET is vulnerable to many attacks like black hole attack, worm hole attack, flooding attack, Sybil attack. In this paper, we focused our attention on black hole attack and proposed a solution for securing the data packets from black hole attack using watch dog.

The remaining of this paper is organized as follows: Section II will be devoted to the general model of watch dog. Section III focuses on black hole attack and protocols. Section IV will be dedicated to summarize other surveys on black hole attack. Section V will focus specifically on the proposed approach of using watch dog against black hole attack. Section VI will be dedicated for simulation results. We close our work in section VII with conclusions and suggestions for future work.

II. GENERAL CONCEPT OF WATCH DOG

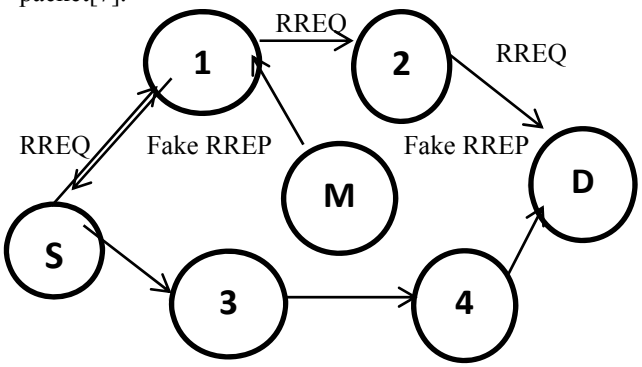
In MANET, the data packet from the source node will be forwarded to the next node until it reaches the destination. In black hole attack, the malicious node in the route will absorb the data packets from source node and will either drop or do not forward it to the next node, thus disconnecting the source node with the destination. Watch dog is a monitoring mechanism that is used to detect the misbehaving nodes in the network[2]. It operates on the property that is broadcasted in wireless sensor networks.

The watch dog maintains a buffer which contains the recently sent data packet to the next node. It monitors for every node and ensures that the same packet is forwarded throughout the route by listening the nodes promiscuously[3]. When any node fails to do so, it is considered as malicious node. Using watch dog, the problems like finding the malicious node, limited power transfer, impartial removal and node conspiracy was solved.

III. BLACK HOLE ATTACK

MANETs are vulnerable to many attacks. Black hole attack is one of the serious attack. When the source node sends for route request(RREQ), the malicious node will advertise itself as having the shortest route to the destination by sending the reply(RREP) with the smallest sequence number. The source node will assume this route to be the shortest fresh route and start forwarding the data packets in this route[4]. Thus, the malicious node acts as a neighbor node and absorbs all data packets from source node and drops the packets, thus disconnecting the source with the destination node[5]. In black hole attack, the malicious node can be placed either next to the source node or anywhere in the route to the destination. They can either be present as a single node or as group nodes forming co-operative black hole attack.

We have used Dynamic Source Routing (DSR) protocol, which is an on-demand source routing protocol. This protocols uses route discovery process to find the route to the destination node. Then, through route maintenance process, the operation of the route is maintained[6]. In this, every packet will carry the list of nodes that it will traverse to reach the destination. The reply from destination node is verified by every node. The identity of the node is verified in the list before it is forwarded to the next neighbor node, else it drops the data packet[7].



S-source node D-destination node M-malicious node 1,2,3,4 – intermediate nodes

Fig 1 Formation of black hole attack (Malicious node)

IV. LITERATURE SURVEY

In [8], Reshma et al has proposed a solution using collaborative watch dog with log file system to detect selfish nodes. With the help of log file system, the overall detection time of finding selfish node is reduced. In [9], Gajendra et al has proposed a solution to provide security in wireless sensor network with two tier architecture which involves three different type of nodes. The sensor nodes which senses the surrounding data, the storage node stores the data and sink node queries the obtained data. In [10], Forootaninia et al has used energy consumption in the functional areas of the wireless sensor network, with the regional and cluster head nodes. They work efficient in sensor nodes life duration.

In [11], Kim et al has proposed an algebraic watch dog which enables to detect malicious behavior and overheard messages. In [12], Lei Huang et al has proposed a solution using extended watch dog mechanism where the system model is created using CTS and RTS. In that, the information sent is not only overheard by its neighbor but also, all the neighbors involved in communication can hear the message communication. The malicious node is identified when the node's dropping rate reaches threshold's value. In [13], Mohammed Reza et al has proposed a solution using watch dog with leach protocol. In this watch dog nodes are selected spontaneously and combined with leach protocol in set up phase and their behavior is studied through steady phase using cluster heads.

V. PROPOSED SOLUTION

In our approach, a sample data is sent from source node to the destination node in all the available routes periodically. Destination node will broad cast the received details to watch dog. A routing table is maintained by watch dog with route Id, size of data sent, size of data received, failure count and continuous/not. Watch dog identifies the malicious node within a specified time interval in each route. The accumulation of response data from destination helps watch dog to decide whether that route has malicious node or not.

When the data loss is continuous, then watch dog identifies the presence of malicious node in that route and deletes the route from the table. Else, the data loss threshold value is used by watch dog to find malicious node's route. The advantage of this approach is, using watch dog, we detect the data loss not only in single route, but also in all the available routes. The watch dog does not waste time in waiting for the reply from destination node from each route, since the sample data is sent periodically in all the routes. One more advantage is, unlike other watch dog process, it accumulates the data count sent and received for specified number of times and uses the same for finding the malicious node in the particular route. This approach helps in avoiding unwanted over load of watch dog.

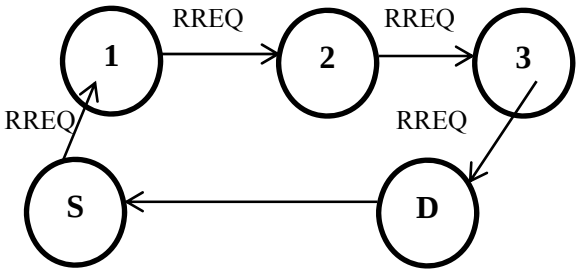


Fig 2 Data transfer mechanism

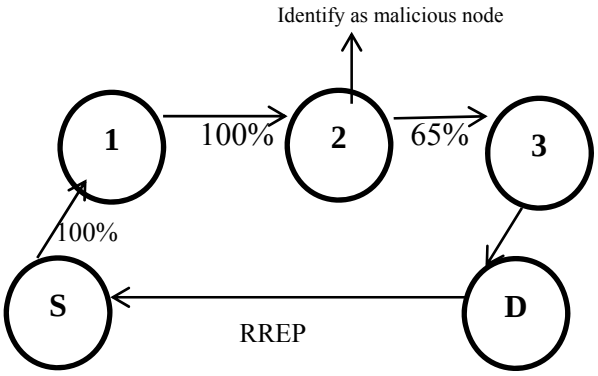


Fig 3 Checking the data loss with Improvised Watchdog

VI. PROPOSED ALGORITHM FOR MALICIOUS NODE DETECTION (IMPROVISED WATCH DOG)

Step-1: Consider a network with N elements.

Step-2: N_i watches a function 'f' over a stream of sample data.

Step-3: The data is treated as discrete time series (for the loss of data).

Step-4: Stream of sample data is sent and watched by N_i until time 't' becomes 5ms (say).

Step-5: Watch dog watches the accumulated set of data values on a stream (with the help of destination node) is denoted by $w_i = (X_i^{t-k+1},\ldots X_i^t)$.

Step-6: Function 'f' is defined as $f(W_i)$. At time interval, 't', if $f(W_i)$ exceeds threshold value $\bar{\iota}_i$, watch dog identifies that node as malicious.

Step-7: Therefore the watch dog event in a network is a random variable, R_i such that,

$$R_i = \begin{cases} 0, \text{ if } f(W_i) >= \bar{\iota}_i \\ 1, \text{ otherwise} \end{cases}$$

VII. SIMULATION RESULTS

We have used NS-2.34 for our simulation, to calculate the number of packet drops and delay in forwarding the data packets. The routing table contains the following columns.

TABLE I
ROUTING TABLE TO IDENTIFY THE DATA LOSS

Route Id	Size of Data Sent	Size of Data Received	Failure Count	Continuous/ Not
1	1024	998	1	Yes
3	900	900	0	No
5	1590	1500	1	Yes
7	1350	1350	0	No

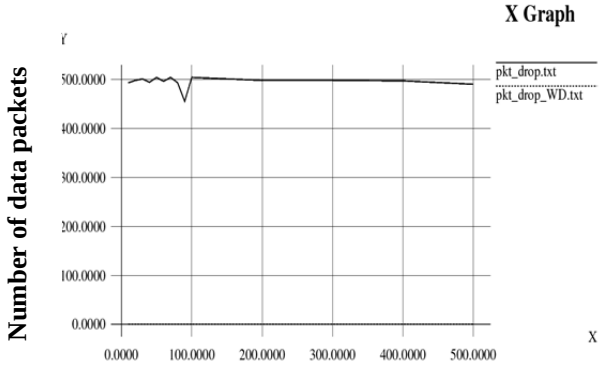


Fig 4 Packet Drop

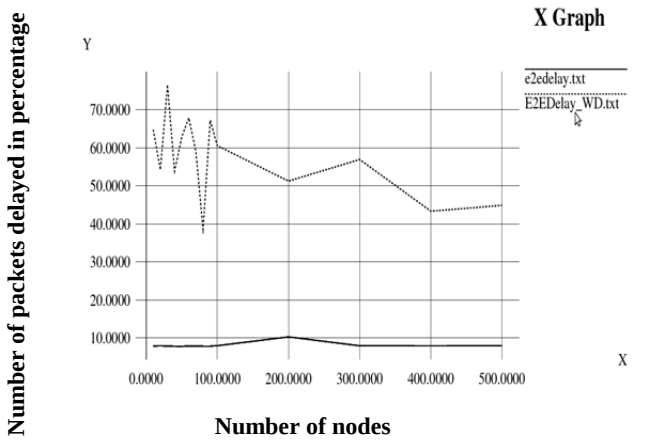


Fig 5 End- to- end Delay

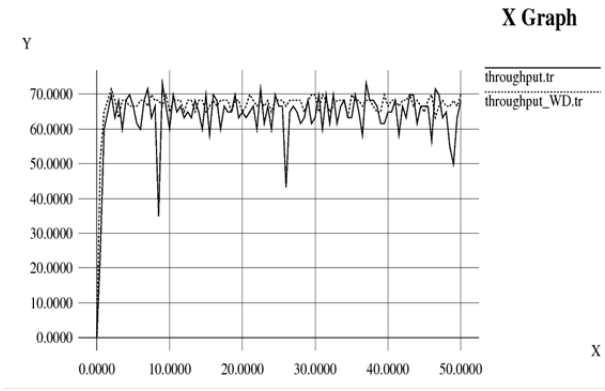


Fig 6 Through

With the above Fig-4, We can observe the number of packet drops are more for 100 nodes and further there is a consistent packet drops for the entire 500 nodes. But, with the improvised watchdog, there is no packet drops at all, because for every node, watchdog confirms and forwards the packets only with the trustworthy nodes. Thus all the packets from source to destination is sent successfully without any packet drop.

The above Fig-5 shows that there is a constant delay from the initial state to the destination in a normal form of forwarding data packets. But after using Improvised watchdog, we can observe that, for the initial 100 nodes, there is a fluctuation in delay and for the rest of the nodes, the delay reduces in a large amount till it reaches the destination. The fluctuation is due to the parameters we have used during simulation which is an expected delay.

The above Fig-6 shows the throughput rates for various number of nodes. The average rate of successful packet delivered is not consistent without using watch dog. But after using watch dog, the throughput rates indicate that the packets are successfully delivered. We can observe the fluctuations which is due to the various parameters that is used during simulation.

VII. CONCLUSION AND FUTURE ENHANCEMENTS

Our proposed Improvised watch dog mechanism has shown efficient results in identifying the malicious node in the route. Using this method, the presence of malicious node in any available path to the destination is identified and within a short period of time, the packets are forwarded without any packet drops and a very less delay. The same concept can be used to calculate other parameters also in future.

REFERENCES

[1] Amit Shrivastava and Nitin chander, "*Overview of routing protocols in MANET's and enhancements in reactive Protocols"*.

[2] Jijeesh Baburajan and Jignesh Prajapati, "*A review paper on watchdog mechanism in wireless sensor network to eliminate false malicious node detection"* , *IJRET*.

[3] Sergio Marti, T.J. Giuli, Kevin Lai, "*Mitigating routing misbehavior in Mobile Ad-hoc Networks*", *(*Mobicom 2000), Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, pages 255-265, New York, NY, USA, 2000, ACM.

[4] Sheenu Sharma and Roopam Gupta, "*Simulation study of black hole attack in Mobile Ad-hoc Networks*" , JEST, 2009, Vol-4, No-2, pg:243-250.

[5] Nishanth Sitapara and Sandeep B. Vanjale, "*Detection and prevention of black hole attack in Mobile Ad-hoc Network"*, Proceedings of ICETE, 2010.

[6] David B. Johnson and David A. Maltz, "*Dynamic Source Routing in Ad-hoc wireless networks"*.

[7] D.Johnson and D.Maltz, "*Dynamic source and routing in wireless ad-hoc networks"*, Mobile Computing Kluwer Academic Publishers,1996.

[8] Reshma Lill Mathew and P. Petchimuthu, "*Detecting selfish nodes in MANETs using collaborative watch dogs*", *IJARCSSE, Vol-3,* Issue-3, 2013.

[9] Gajendra Singh and Monali V. Ghode, "*Advanced security mechanism in wireless sensor network using watch dog and SAFEQ mechanism"*, IJSR.

[10] A. Forootaninia and M.B. Ghaznavi – Ghoushchi, "*An improved watch dog technique based on power aware hierarchial design for IDS in wireless sensor networks*", IJNSA, Vol-4, No-4, 2012.

[11] Kim, Minji, Muriel Medard and Joao Barros, "*Algebraic watch dog-mitigating misbehavior in wireless network coding* ", IEEE Journal on selected areas in communication – 2011.

[12] Lei Huang and Lixiang Liu, "Extended Watch dog Mechanism for Wireless Sensor Networks", JICS, Vol-3, No-1, 2008.

[13] Mohammed Reza Rohbanian, Mohammed Rafi Kharazmi, Alireza Keshavarz-Haddad and Manije Keshtgary, "Watch dog-LEACH: A New Method Based on LEACH Protocol to Secure Clustered Wireless Sensor Networks".

[14] Network simulator, www.isi.edu/nsnam/ns.