Watchdog: A Study on Examining and Eliminating Misbehavior

Saurabh Bora
Uttarakhand Technical University
Haldwani, Uttarakhand
India

Shivendra Singh
Uttarakhand Technical University
Pithoragarh, Uttarakhand
India

Sheikh Mohamad Arsalan
Uttarakhand Technical University
Srinagar, Kashmir
India

Anchit Bijalwan
Uttarakhand Technical University
Dehradun, Uttarakhand
India

ABSTARCT
WSN is a mechanism which is widely deployed for data monitoring in industrial, commercial and many other fields (like military etc.). Many of research have generally focused on making the network feasible and as useful as possible, but in the advent of this the security was given a very less priority and no attention was given to its security. These WSN networks face a wide variety of threats like the wormholes, grey hole attack, message tampering and selective forwarding etc. WSN are mainly attacked by the malicious packet drops. Now talking about the MANET (Mobile Ad hoc Networking) which is defined as the collection of wireless mobile nodes. MANET forms a network without using any of the infrastructures. The algorithm used to overcome this problem is the watchdog algorithm, but the watchdog algorithm has a partial drop problem, in this partial drop problem the attacker can manipulate the packet dropping rate below the threshold. Watchdog does not consider the traffic situations; these situations include congestion and collision. Through this article we have tried to eliminate the drawbacks of the watchdog algorithm. This paper proposes four theories for eliminating drawbacks of the watchdog.

Keywords
Halt, Acknowledgement, Numbering, Detection Graph

1. INTRODUCTION
Watchdog algorithm is a checking mechanism which acts as a trust system for most of the Ad Hoc and WSN. Research shows that current watchdog mechanism evaluates only the next HOP behaviour of the node, and then broadcasts or propagates the evaluation result to the adjacent node. This propagated result is neither energy efficient nor attack resistant. Watchdog detects the malicious misbehaving of nodes by listening to the next Hop transmission. In certain cases watchdog may overhear that its next node has failed to forward the packet within a certain amount of time period, the Watchdog increases the failure counter .When the malicious node exceeds the failure counter then predefined threshold, then the watchdog reports it as misbehaving node.

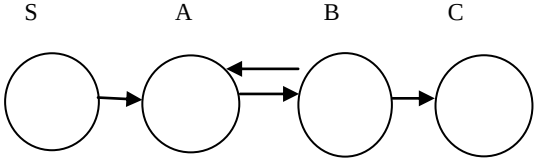

Figure 1. Packet Transfer Mechanism

The above figures shows how the packets are transferred from one node to the other .The above diagram also show the working of the watchdog algorithm. As it can be seen that A cannot directly transmit the packet to node C .So node A uses node B to forward the packet to C.A can check whether node B has transmitted the packet to node C or not. One can implement the watchdog algorithm in this case, by maintaining a buffer of the all the recently sent packets and match them afterwards with the overheard packets to see whether there is a match or not. If the match is found then the packet is deleted from the buffer as it has been forwarded on. If any of the packets defined in the buffer remains for a long time, the watchdog increments a tally known as the failure tally for the node responsible for forwarding that packet .If the tally exceeds a certain amount of threshold bandwidth, the watchdog determines that node responsible for forwarding as misbehaving and sends a message to the source determining that it's a misbehaving node. The Limitations of Watchdog algorithm are AMBIGOUS COLLISION, RECIEVER COLLISION, LIMITED TRANSMISSION POWER, FALSE MISBEHAVIOUR and PARTIAL DROPPING.

In this paper we examined the watchdog algorithm. In this it can be analyzed that there are some drawbacks to it and we somehow tried to overcome it by certain theories. This article has been categorized into five sections. In section 2 there is a LITERATURE SURVEY which deals with a survey of many researchers and their valuable approach. In section 3 there is an examination of the watchdog algorithm and certain drawbacks of the watchdog algorithm. In section 4, there are some theories which will help to improve the current existing watchdog algorithm. Last is the CONCLUSION which is in section 5.

2. LITERATURE SURVEY:
Graffi et al., [1] conducted mechanism for misbehaving nodes in the network which was proposed to detect colluding misbehaviour on the nodes. The solution was by applying a leak detector. It was a simple and low cost idea approach as there is no need of using or going through cryptography as compared to F.Kargl [2] idea which is howsoever costly as it goes by iterative probing which is somehow infeasible. In leak detector algorithm there were some assumptions. The main idea of Leak Detector is that the destination node of a route builds up a virtual graph, which models the multipath from the source node to the destination node.

A.Babu et al., [3] proposed a similar mechanism for misbehaviour in nodes for eliminating false malicious nodes in the network and applied Change Point Detection algorithm. The objective was to improve existing watchdog algorithm by exactly detecting the malicious node in the network.

Kim et al., [4] proposed a mechanism known as algebraic watchdog in which it enables the node to detect malicious behaviour and overheard messages to police to downstream neighbour locally. It also delivers a secure global self-checking network (unlike BYZANTINE Detection protocol).

S.Sujata et al., [7] proposed a theory for eliminating misbehaviour nodes in network. She used TWOACK and AACK approaches in this reference.

Huang et al., [8] eliminated limitations of watchdog algorithm by introducing threshold mechanism.

S.Matri et al., [9] proposed to trace malicious nodes by using Pathrater.

Gonzalez et al., [10] presents a methodology, for detecting packet forwarding misbehaviour, which is based on the principle of flow conservation in a network.

3. EXAMINATION OF WATCHDOG ALGORITHM

Watchdog algorithm is basically used for secure delivery of packets through different nodes in a network. It helps in identifying the misbehaving nodes in a network. In this all the nodes in a network has their own watchdog which study the behavior of its neighboring node and thereby telling whether packet is going to next node or not. In Fig 2. S sends data to A. Now A will have its watchdog and so will S. As soon as A forwards data to B, S will overhear that packet has been arrived from A. But watchdog comes with certain drawbacks [6][3] which hinder it from detecting malicious nodes. These drawbacks include:

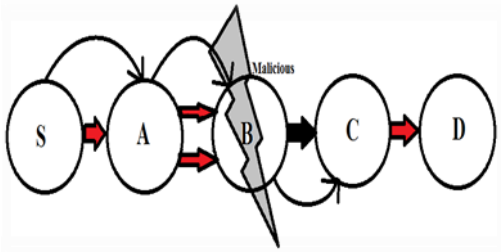

Figure 2. Watchdog Mechanism

• **Ambigous Collision:** Consider a case that A sends data to B. When B sends data further to C then A should overhear but if at same time A receives data from some other source. In such a case A will not overhear and hence B will be considered as malicious, which is untrue. So this is a limitation as in spite of not being malicious B is considered to be.

• **Reciever Collision:** Now consider a case in which B sends data to C which isn't received. In such a case A may overhear that B has forwarded the data but is unaware and can't tell that whether it's received or not.

• **Limited Transmission Power***:* If A overhears that B has sent data but C did not receive and if B can adjust its transmission power then it may drop data in between and prove to be malicious.

•**False Misbehavior***:* In this a malicious node intentionally claims that other nodes are malicious and misbehaving. If B is malicious then it will claim that A is misbehaving or C is misbehaving although they are not. In this case 2 nodes that are not neighbour consider each other as malicious.

•**Partial Dropping:** In this case although node is B is transferring data to C but partial data. Means whatever A sends B forward it to C but some part of packet is dropped out and only some part is received by C such that failure tally will not exceed threshold of A's watchdog.

4. PROPOSED WORK

The purpose is to improve the existing watchdog algorithm by mainly removing all its given drawbacks:

1) HALT: This concept is basically used to remove the ambiguous collision in which a sender node is not able to overhear from receiver node receiving the packet due to traffic from other nodes at its end. This mechanism can be used to halt the process of the sender end till it receives the acknowledgment from the receiver node which otherwise can be considered as malicious. The halting of the process would not allow other neighboring nodes of sender to send packets while it is receiving acknowledgment from the receiver. Halt mechanism helps in removing the core disadvantage of the Watchdog algorithm. For example node B is sending packets to node C. While acknowledgment is being received from node C to node B it halts the process so that it overhears the transmission from node C to node B and not considers it malicious. It allows it not to get mislead while others are sending packets to it and receive the acknowledgment.

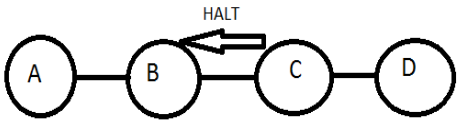

Figure 3. Halt Mechanism

2) ACKNOWLEDGMENT: - The main idea behind this concept is to remove the two main disadvantages of the watchdog algorithm receiver collision and limited transmission power. In both of these when for example node A sends a packet to node B then it sends the packet to node C. When node B sends the packet to node C node A overhears that node C has received the packet due to some other sender node X sending packet to node C this causes receiver collision. The same problem arises when node A overhears node C of receiving the packets then node B can drop the packets this causes limited transmission power. In this concept a packet that will act as reverse for the two hops to carry the acknowdgment whether node C has received the packets send from node A or not. This mechanism helps us to remove these two disadvantages and increasing the accuracy of the watchdog.

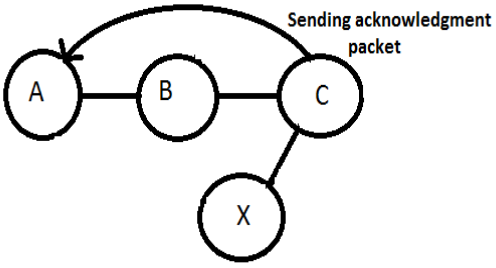

Figure 4. Acknowledgement Mechanism

3) NUMBERING: - This concept helps us to remove the false misbehavior and helps us to improve the efficiency of the algorithm. In this we increment the counter in each node

when it successfully transmits the packet to the next node if the node does not transfer the packet then the value of that node will not be incremented and it will remain zero. Thus by detecting the no of nodes that have zero value helps us to detect the malicious nodes in the watchdog algorithm. This helps us to remove one of the complex disadvantage in which a node misbehaves and gives the wrong information to the sender about the node which is not in contact with it. Thus allowing sender to consider it as a malicious node.

4) DETECTION GRAPH: - This idea helps us to remove colluding and partial dropping in the watchdog algorithm. In this we have a sender and a receiver which maintain all the traffic rate .The amount data send from the sender and received are all maintained. So when a malicious node drops some packets as in partial dropping or in colluding the destination node receives the packets and checks it with the inflow send from the sender. Thus by detecting the path followed and the amount of incoming and outgoing packets in each node the malicious node can be detected. The destination node plays a crucial role in detecting the malicious node by maintaining the deviation in the outflow and the inflow at each node.

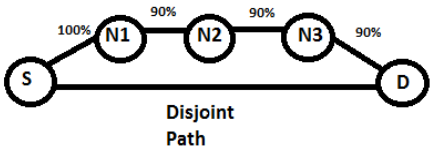

Figure 5. Detection Graph

In this fig (5) it can be concluded that destination maintains the traffic of inflow and outflow in the given nodes through a disjoint path. As the rate of outflow is less in node N1 to the rate of inflow it can be considered to be malicious by using this mechanism of detection graph.

5. CONCLUSION

There is a must need of detecting malicious node as it can manipulate the whole result and loss of data packets. This paper has tried to eliminate disadvantages of current wireless LAN network by some methodologies. The future scope of this paper is to prevent data loss, tampering of useful data and eliminate malicious node. By implementing some techniques as halt**,** acknowledgment**,** numbering**,** and detection graph and somehow tried to improve existing watchdog algorithm.

6. REFRENCES

[1] K´alm´an Graffi, Parag S. Mogre, Matthias Hollick, and Ralf Steinmetz , "Detection of Colluding Misbehaving Nodes in Mobile Ad hoc and Wireless Mesh Networks," in IEEE GLOBECOM, November 2007.

[2] F. Kargl et al., "Advanced Detection of Selfish or Malicious Nodes in Ad Hoc Networks," in Proceedings of ESAS '04, 2004.

[3] A.Babu Karuppiah, T.Meenakshi, T.I.Mano Ranjitha & S.Vivitha, "False Misbehaviour Elimination in Watchdog Monitoring System Using Change Point In a Wireless Sensor Network," in GRET.

[4] Kim, MinJi, Muriel Medard, and Joao Barros. "Algebraic Watchdog: Mitigating Misbehaviour in Wireless Network Coding."IEEE Journal on Selected Areas in Communications 29.10(2011)

[5] H. Yang, J. Shu, X. Meng, and S. Lu, ―SCAN: Self-organized network layer security in mobile ad hoc networks, IEEE Journal on Selected Areas in Communications, vol. 24, issue 2, pp. 261-273, February 06.

[6] 6-Youngho Cho and Gang Qu, Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks, IEEE Symposium on Security and Privacy Workshops, 2012.

[7] S.Sujatha, B.Lakshmi Radhika, "A Study On Enhanced Adaptive Acknowledge (EAACK) Scheme In Receiver Collisions – An IDS In Wireless Mobile Ad-Hoc Networks," in The International Journal Of Engineering And Science (IJES).

[8] Extended Watchdog Mechanism for Wireless Sensor Networks Lei Huang, Lixiang Liu, Journal of Information and Computing Science, 2007.

[9] S. Matri, T. J. Giuli, K. Lai and M. Baker, Mitigating Routing misbehaviour in Mobile Ad Hoc Networks. Proceedings of the 6th annual international conference on Mobile Computing and Networking (MOBICOM), Boston, Massachusetts, United States, 2000, 255-265.

[10] Oscar F. Gonzalez, Michael Howarth, and George Pavlou, Detection of Packet Forwarding Misbehaviour in Mobile Ad-Hoc Networks.Center for Communications Systems Research, University of Surrey, Guildford, UK.Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.

[11] Komala CR, Srinivas Shetty, Padmashree S., Elevarasi E., ―Wireless Ad hoc Mobile Networks, National Conference on Computing Communication and Technology, pp. 168-174, 2010.

[12] F. Anjum, Anup K. Ghosh, Nada Golmie, Paul lodzy, Radha Poovendran, Rajeev Shorey, D. Lee, J-Sac, ―Security in Wireless Ad hoc Networks, IEEE journal on selected areas in communications, vol. 24, no. 2, February 2006.