Detection of Black Holes in MANET Using Collaborative Watchdog with Fuzzy Logic

Y. Harold Robinson, M. Rajaram, E. Golden Julie, S. Balaji

***Abstract*—**Mobile ad hoc network (MANET) is a self-configuring network of mobile node connected without wires. A Fuzzy Logic Based Collaborative watchdog approach is used to reduce the detection time of misbehaved nodes and increase the overall truthfulness. This methodology will increase the secure efficient routing by detecting the Black Holes attacks. The simulation results proved that this method improved the energy, reduced the delay and also improved the overall performance of the detecting black hole attacks in MANET.

***Keywords*—**MANET, collaborative watchdog, fuzzy logic, AODV.

I. Introduction

MANET has the collection of autonomous mobile nodes that communicate over the wireless link with the infrastructure less network. Functioning of ad-hoc network is dependent on the cooperation and trust values of the nodes. Nodes can convey the information about the topology of the network with the neighbor nodes. The primary challenge in building an Ad-hoc network is equipped each device to continuously maintains the information required to the proper route traffic. MANET is highly dynamic and autonomous topology [1].

MANET consists of a peer-to-peer, self-forming and self-healing network. It is vulnerable due to these fundamental characteristics of open medium, dynamic topology, distributed cooperation and constrained capability. The broadcasting method for multipath routing can be done using fuzzy classification [2].Key pre-distribution scheme is playing an important role of detecting black hole in MANET [9]. Opportunistic routing with Coded MAS approach is the alternate routing of detecting black hole attack by generating link failure in MANET. Cryptographic techniques such as encryption and decryption methods for active node in the network can be implemented using the technique discussed in [6]. Trustworthy link failure algorithm is implemented in wireless networks to find the link failure in the active wireless networks [5]. Energy aware Particle Swarm Optimization techniques can be implemented in MANET for improving quality of service [3].

Security in MANET is a big challenge; it has no centralized ability which can organize the entity nodes working in MANET [8]. Black hole attack decreases the network performance and reliability. A black hole node sends the route response to the sender and advertises itself having the shortest path to reach its destination [11]. When source node sends the packet to the attacker node, it drops the entire packet without forwarding. Watchdog technique is a monitoring technique; it forwards the packet and listens its neighbor node which in its transmission range [10]. A collaborative approach for detecting the black holes and selfish nodes in MANET were using a set of watchdog which collaborates to increase their individual and collective performance. Fuzzy logic is the form of many-valued logic, the truth values may be a real number between 0 and 1 [7]. Discovery of preeminent route simply based on power complementary deliberation might direct to lengthy path among elevated interruption and diminish system generation time [12].

II. Literature Review

Channel allocation for dynamic wireless networks was developed in the existing techniques in [8]. Ad hoc on-demand distance vector routing protocol is a reactive protocol which creates a way from source node to destination node as soon as required and is a conversion of the DSDV protocol for active connection conditions. It supports both unicast and multicast routing. In AODV a route is created only on demand when new node needs a connection then it broadcasts a request for connection. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available in rate adaption technique [4]. If it is available, it uses a route to send packets to destination. If it is not available or previously entered packet is inactivated then the node initiates the route discovery process. A RREQ packet is broadcast by the node. Every node receives RREQ packet first if it is the destination for the packet; then, it sends back an RRES packet [12]. If it is not the destination; then, it checks the routing table to determine if it has a route to the destination. Before forwarding the packet, all nodes can steadfastness gather transmit symbol and also the preceding node symbol. If no reply is received for the request, then the intermediate nodes have using the timer to delete the entry. If the reply is received for request, the intermediate nodes will keep the broadcast identifier and the previous nodes from which the reply came from [11]. The transmit identifier number and source identifier are needed to sense the node has collected the route request communication or not. All destinations will become unreachable due to loss of link. Once

Harold Robinson Y. and BalajiS.are Associate Professors with the Department of Computer Science and Engineering, SCAD College of Engineering and Technology, India (e-mail: yhrobinphd@gmail.com, sbalajiphd@gmail.com).

Prof. Dr. M. Rajaram is the Vice-Chancellor, Anna University Chennai, India (e-mail: rajaramgct@rediffmail.com)

Golden Julie is an Assistant Professor, Department of Computer Science and Engineering, Anna University, Chennai, India (e-mail: goldenjuliephd@gmail.com).

the source receives the RERR, it reinitiates route discovery if it still requires the route [10].

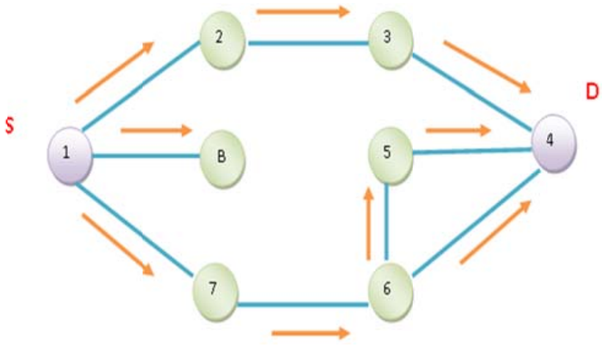

Fig. 1 RREQ from source to all nodes

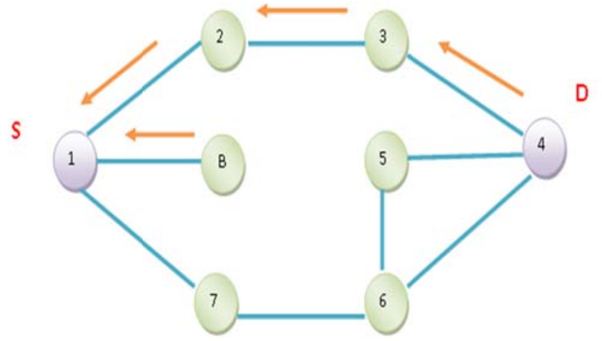

Fig. 2 RRES Replying

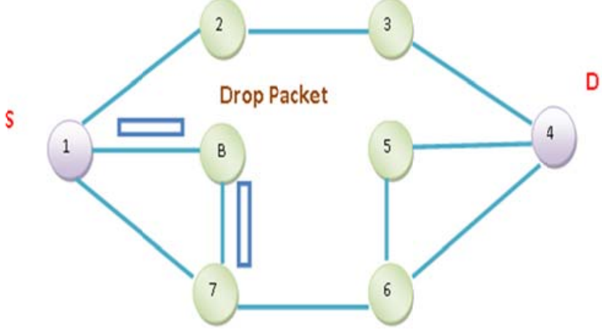

Fig. 3 Blackhole Attack

In Fig. 1, S (node 1) is a source node and D (node 4) is destination node. S wants to establish a connection to D. S sends route request message to its neighbor nodes. Neighbor node checks its routing table if the path found sends reply otherwise it forwards the RREQ message to its neighbor. This process will continue until the destination node or proper route path is not found. In Fig. 2, S has two shortest ways, initial is D causing the RREP message having shortest path and second is part node B causing RREP message having shortest path. B pretends because it has terribly shortest path however it's not contains a correct routing path to D and conjointly it sends the RREP message initial than the opposite nodes in order that the S sends the information packet to B. And, B is dropping all packets without forwarding it to destination D. Fig. 3 shows the scenario of Black hole attack, node B drops the packet of node S. Attack comes from both inside and outside network.

TABLE I
TYPES OF ATTACKS

LAYER	ATTACK
APPLICATION LAYER	negation, Data sleaze
TRANSPORT LAYER	Session seize, SYN inundation
NETWORK LAYER	Worm hole attack, Black hole attack
DATALINK LAYER	Traffic investigation ,distraction
PHYSICAL LAYER	snoop, interceptions, jamming

Black Hole Attack might be a fairly denial of service attack where a malicious node can attack all the packets by incorrectly claiming a recent route to the destination. A black hole attack is referred to as node dropping all packets and sending forged routing packets over itself. If the attacking node is a connecting node of two components of that network, then it effectively separates the network into two disconnected components.

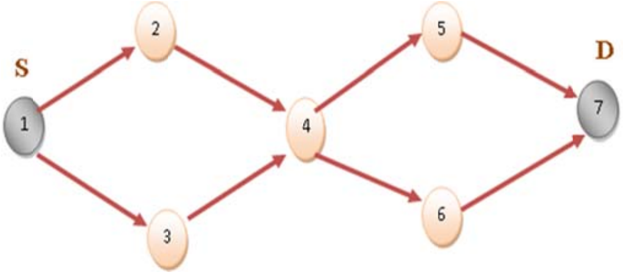

Fig. 4 Path from source to destination

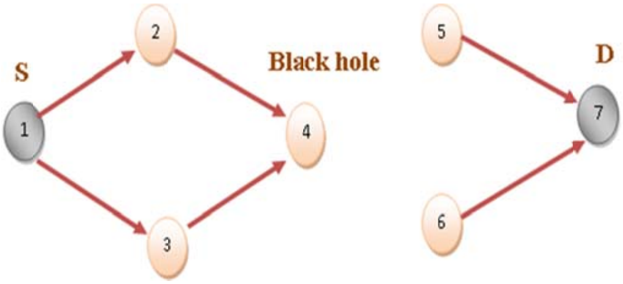

Fig. 5 Black hole separates the nodes

III. PROPOSED WORK

Watchdog must be considered as an intrusion detection system, which collects and analyzes the network traffic to detect a set of attack. It aims to monitor the activity of nodes in order to detect the misbehavior of nodes.

A. Bayesian Watchdog

To detect misbehaved nodes, network monitoring is needed. Every node must be aware of its neighbor's behavior, and watchdogs are a popular component for intrusion detection system dedicated to this task. The main problem is that watchdogs are characterized by a significance amount of false positives, basically due to mobility and signal noise. Previous works from have evaluated a Bayesian watchdog [4] over Ad-hoc On-demand Distance Vector (AODV) routing in MANETs. This Bayesian watchdog results from the aggregation of a Bayesian filter with a standard watchdog implementation. The standard watchdog simply overhears the packets transmitted and received by its neighbors, counting the packets that should be retransmitted, and computing a trust level for every neighbor. If a node retransmits all the packets that it should have retransmitted, it has a trust level of 1. If a node has a trust level lower than the configured tolerance threshold, that node is marked as malicious. The role of the Bayesian filter in the watchdog is to probabilistically estimate a system's state from noisy observations**.**

The mathematical foundation of the Bayesian filter is the following: At time t, the state is estimated by a random variable υ, which is unknown, and this uncertainty is modeled by assuming that it is drawn according to a distribution that is updated as new observations become available. It is commonly called *belief* or $Bel_t(\upsilon)$. To illustrate this, let's assume that there is a sequence of time-indexed observations $z_1, z_2, ..., z_n, ..., z_t$. The $Bel_t(\upsilon)$ is then defined by the posterior density over the random variable j conditioned on all sensor data available at time t:

$$Bel_t(\upsilon) = p(j|z_1, z_2, ..., z_n, ..., z_t) = Beta(\alpha_t, \beta_t, \upsilon) \quad (1)$$

In this approach, the random variable υ belongs to the interval [0,1]. Bayesian filtering relies on the Beta distribution, which is suitable to estimate the belief in this interval. α and β represent the state of the system, and they are updated according to:

$$\alpha_{t+1} = \alpha_t + z_t \quad (2)$$

$$\beta_{t+1} = \beta_t + z_t \quad (3)$$

The Beta function only requires two parameters that are continuously updated as observations are made or reported. In this approach, the observation z_t represents the information from the local watchdog obtained in time interval [t, t + δt] about the percentage of non-forwarded packets. The Bayesian watchdog uses three parameters: The first two parameters are α and β, which are handled over to the Beta function to obtain an estimation of the node's maliciousness. Thus, we can say that α and β are the numeric representation of a node's reputation. The third parameter is g, which represents the devaluation that old observations must suffer to adapt the watchdog's behavior to a continuously changing scenario without penalizing certain nodes forever. It is a mechanism to reintegrate nodes into the MANET if they change their behavior to a more cooperative one.

B. Collaborative Watchdog

A collaborative Bayesian watchdog is based on a message-passing mechanism in every individual watchdog that allows publishing both self and neighbor reputations. The underlying idea of our approach is that if a Bayesian watchdog works well for detecting black holes, a group of collaborating neighboring Bayesian watchdogs would be able to perform faster and more accurate detections.

Similar to the Bayesian watchdog, the collaborative Bayesian watchdog overhears the network to collect information about the packets that its neighbors send and receive. Additionally, it obtains α and β values for its whole neighborhood. These values are obtained by the Bayesian watchdog with the same observations; we call them 'first hand information' or 'direct reputations'. Periodically, the watchdog shares these data with its neighbors, and we call them 'second hand information' or 'indirect reputation'. In our implementation, indirect reputations are modulated using a parameter δ.

$$\alpha(i)^1_j = (\alpha(i)_j + \delta.mean(\alpha(i)^k_j) / 2 \quad (4)$$

$$B(i)^1_j = (\beta(i)_j + \delta.mean (\beta(i)^k_j) / 2 \quad (5)$$

i is the node which is performing detection; Ni is the neighborhood of node i; $\alpha(i)j$ is the value of a calculated for every neighbor j of i, obtained from direct observations at i; $\beta(i)j$ is the value of b calculated for every neighbor j of i, obtained from direct observations at i; $\alpha(i)^k j$ is the value of a calculated for every neighbor j of i, obtained from observations of every neighbor k of j; $\beta(i)^k j$ is the value of b calculated for every neighbor j of i, obtained from observations of every neighbors k of j; δ represents the level of trust or the relative importance that a neighbor's observed reputations have for node i.

When indirect reputations arrive at a node from one of its neighbors, it only processes those reputations for its own neighbors, because reputations about nodes that are not in its neighborhood are useless. Once the reputations have been obtained, and the adequate analysis has been done, the detection only needs a predefined tolerance threshold to identify if a node is misbehaved or not.

First, each individual watchdog overhears the network to make direct observations of its neighbors, thereby detecting black holes as the Bayesian watchdog does. Periodically, it receives reputation information from its neighbors and evaluates their behavior taking into account this second hand information and its direct observations.

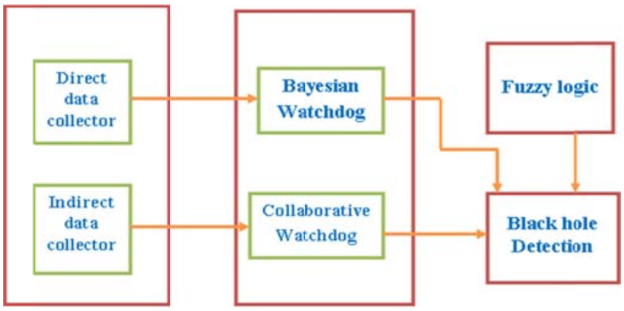

Fig. 6 Architecture of collaborative watchdog with fuzzy logic

The Bayesian Detection function performs investigation over straight clarification, obtaining the values of α and β. The connection between α and β exceeds a predefined forbearance altitude, the watchdog identifies that node as malicious. These values of α and β are also used in the Collaborative Detection function according to (4) and (5).

C. Fuzzy Logic

Fuzzy Logic has to handle the concept of partial truth where the trust values range between completely true or completely false. Both degrees of truth and probabilities range between 0 and 1. Fuzzification operation can map input values into fuzzy membership function. Defuzzifying operation can be used to map a fuzzy output membership function into a crisp output value that can be used for decision or control purpose.

In Fuzzy Logic System, weightings can be optionally added to each rule in rule base and used to regulate the degree to which a rule affect the output rules. Fuzzy logic process:

- Fuzzify all input values into fuzzy member function.
- Execute all applicable rules in the rule base to compute the fuzzy Output function.
- Defuzzifying the fuzzy output function to get crisp output values.

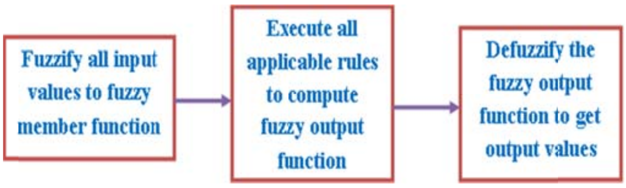
Fuzzify all input values to fuzzy member function
Execute all applicable rules to compute fuzzy output function
Defuzzify the fuzzy output function to get output values

Fig. 7 Fuzzy logic process

TABLE II
REPUTATIONS RECEIVED

Neighbor	Reputations received ({$\alpha(A)^k_j$, $\beta(A)^k_j$})
B	F: {5,1}, G:{11,1}
C	E:{1,4}, G:{18,1}, H:{1,1}
D	E:{1,2}, F:{7,1}
E	C:{34,1}, D:{1,6}, F:{15,1}
F	B:{1,1}, D:{1,4}, E:{1,3}, G:{13,1}
G	B:{1,2}, C:{52,1}, F:{27,1}, H:{1,6}
H	C:{21,2}, G:{2,13}

TABLE III
COLLABORATIVE REPUTATIONS CALCULATED AT A NODE

Neighbour	Reputations	
	Direct	Indirect
B	{1, 2}	{1, 1.5}
C	{43, 1}	{57, 1}
D	{1, 4}	{1, 5}
E	{1, 1}	{1, 3}
F	{1, 4}	{14, 1}
G	{3, 1}	{14, 1}
H	{68, 1}	{44,1}

TABLE IV
DETECTION OF BLACK HOLE ATTACK

({$\alpha(A)^1_j$, $\beta(A)^1_j$})	Black Hole Detection Method	
	Bayesian	Collaborative
{1, 1.75}	No	No
{50, 1}	No	Yes
{1, 4.5}	No	No
{1, 2}	No	No
{7.5, 2.5}	No	No
{8.5, 1}	No	No
{56, 1}	Yes	Yes

IV. BLACK HOLE DETECTOR PROCESSING ALGORITHM

```
Function BayesianDetection()
Get observations
Compute α and β values
If values between α and β greater than tolerance
Then return true
Else return false
EndIf
EndFunction

Function CollaborativeDetection()
Get neighbourhood observation
Compute α’ and β’ values
If values between α’ and β’ greater than tolerance
Then return true
Else return false
EndIf
EndFunction

(fuzzy logic)
Compute the input values
If input values between 0 and 1
Then return True
End If.
```

V. PERFORMANCE EVALUATION

A. Detection Speed

Detection speed is important when detecting the black holes. Accuracy and speed must be well balanced. The watchdog enhancements will target both speed and accuracy issues. In dense networks with traffic load equally balanced between malicious and well-behaved nodes, both watchdog versions will perform nearly equally, despite of the smaller number of packets that the collaborative Bayesian watchdog needs to perform detections. This is because the interval between packets is very short. Nevertheless, in networks with low traffic load and with black holes that transmit a very small amount of packets, the difference of performance between the two approaches could be more in terms of time. Fig. 8 illustrates the analysis of the energy result, Fig. 9 illustrates the analysis of delay result and Fig. 10 illustrates the analysis of ratio result.

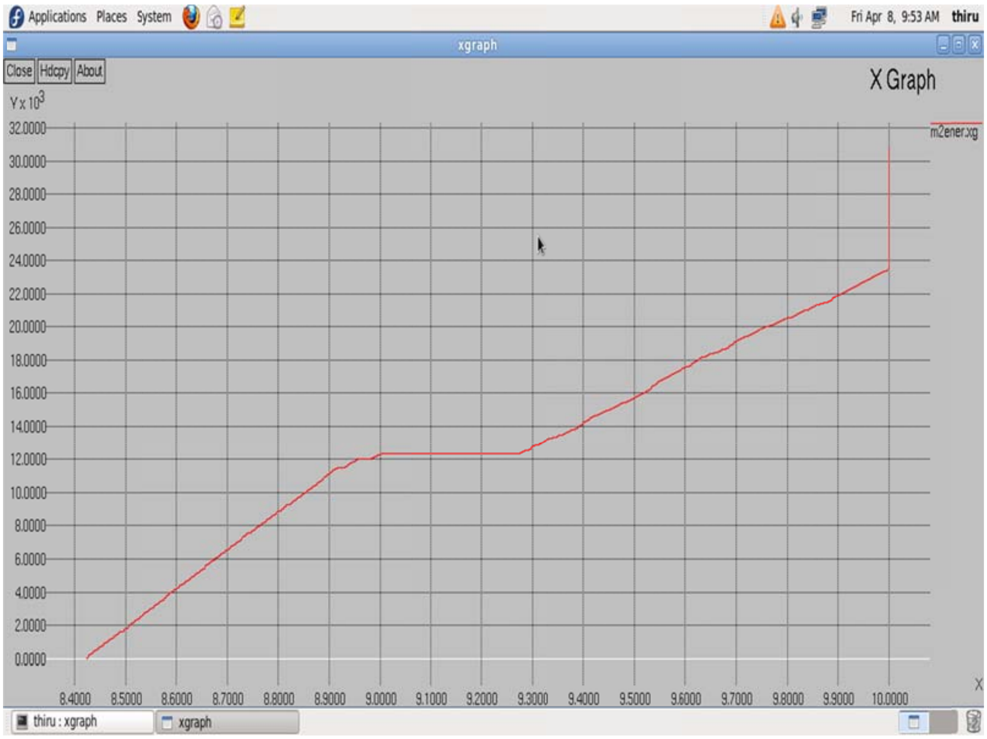

Fig. 8 Analysis of Energy Result

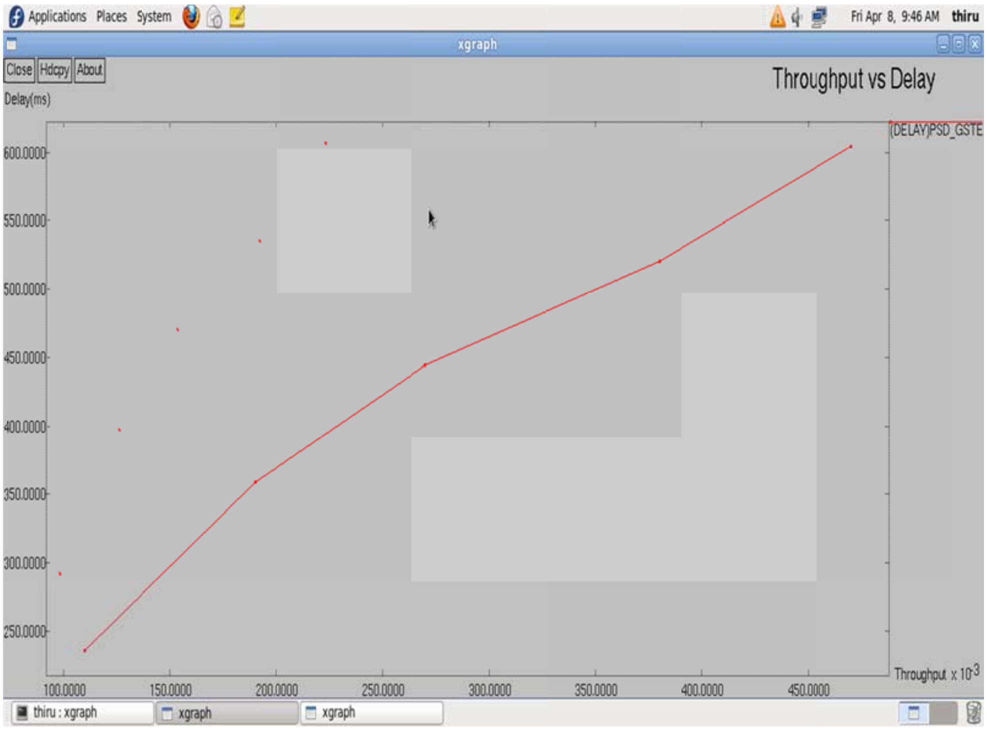

Fig. 9 Analysis of Delay Result

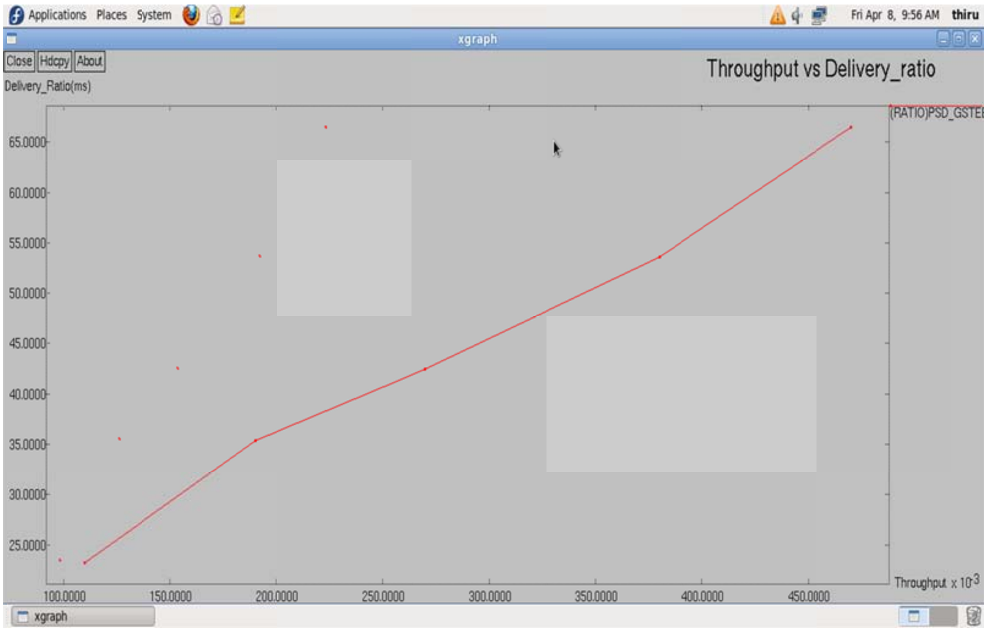

Fig. 10 Analysis of Ratio Result

B. Accuracy

Accuracy in detecting false positives and false negatives is also slightly better than with the non-collaborative Bayesian watchdog, which comes from the decreased level of false negatives. The fact is that a small amount of black holes, which are not detected with the Bayesian watchdog, are now detected by the collaborative Bayesian watchdog. Our approach is able to detect cases where a black hole enters and exits from the range of a watchdog quickly.

VI. Conclusion

This paper showed that a Bayesian watchdog performs better than a standard watchdog, reducing the amount of false positives. Analyzing secondhand information using a collaborative Bayesian watchdog will also help at boosting its performance by decreasing the amount of false negatives and speeding up the detection process. This watchdog technique fits not only generic MANET environments, but also VANET environments.

References

[1] Multi-Node Wireless Energy Charging in Sensor Networks, Liguang Xie, Member, IEEE, Yi Shi, Senior Member, IEEE, Y. Thomas Hou, Fellow, IEEE Wenjing Lou, IEEE, Hanif D. Sherali, and Scott F. Midkiff, April 2015.

[2] Harold Robinson, Y., & Rajaram, M. (2016), "A memory aided broadcast mechanism with fuzzy classification on a device-to-device mobile Ad Hoc network", Wireless Personal Communications, 1–23, doi:10.1007/s11277-016-3213-0.

[3] Harold Robinson, Y., & Rajaram, M. (2015), "Energy-aware multipath routing scheme based on particle swarm optimization in mobile ad hoc networks", The Scientific World Journal, 1–9. doi:10.1155/2015/284276.

[4] Y. T. Hou, Y. Shi, and H. D. Sherali, "Rate allocation and network lifetime problems for wireless sensor networks," IEEE/ACM Trans. Netw., vol. 16, no. 2, pp. 321–334, Apr. 2008.

[5] Harold Robinson, Y., & Rajaram, M. (2015). "Trustworthy link failure recovery algorithm for highly dynamic mobile adhoc networks", World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, vol.9, no.2, 233–236.

[6] Kai Zeng, Wenjing Lou, Jie Yang, Donald R. Brown III, "On Throughput Efficiency of Geographic Opportunistic Routing in Multihop Wireless Networks", *Springer, Mobile Networks Application* (2007) 12:347–357, 2007.

[7] Sanjit Biswas, Robert Morris, "ExOR: opportunistic multi-hop routing for wireless networks", *Proceedings of conference on Applications, technologies, architectures, and protocols for computer communications*, Pages 133-144, 2005

[8] A. Trivino-Cabrera, S. Canadas-Hurtado, "Survey on Opportunistic Routing in Multihop Wireless Networks", *International Journal of Communication Networks and Information Security (IJCNIS),* Vol. 3, No. 2, August 2011.

[9] Harold Robinson, Y., &Rajaram, M. (2015), "Establishing pairwise keys using key Predistribution schemes for sensor networks", World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 9, no.2, pp. 608–612.

[10] D. Boneh, D. Freeman, J. Katz, and B. Waters, "Signing a linear subspace: signature schemes for network coding," in Proc. 2009 PKC, vol. 5443, pp. 68–87.

[11] B. Radunovic, C. Gkantsidis, P. Key, and P. Rodriguez:, "Toward practical opportunistic routing with intrasession network coding for mesh networks," IEEE/ACM Trans. Networking, vol. 18, no. 2, pp. 420–433, 2010.

[12] Ehsan Ahvar, Mohammad Jalil Piran, "SELECTOR: An Intelligent Evaluation System for Routing Protocols in Wireless Ad Hoc and Sensor Networks", Proceeding of 3rd International Conference on Electronics Computer Technology, ICECT 2011, IEEE, Kanyakumari, India, p.p. 300~305, April 8~10, 2011.

Y. Harold Robinson is currently working as an Associate Professor, dept of CSE in SCAD College of engineering and Technology, Tirunelveli. He finished ME degree in Anna University, Chennai. He is Pursuing his Ph.D from Anna University Chennai. His research interests are Wireless networks Mobile Computing, Wireless Sensor Networks. He has published several Research papers in International Journals. He has presented many papers in National and International conferences in Network security, Mobile Computing and Cloud Computing.

Prof. Dr.M. Rajaram M.E., Ph.D is the Vice-Chancellor of Anna University, Chennai. As a research guide, Dr. M. Rajaram produced 30 Ph.D's and four M.S. scholars in various fields. At present, 10 research scholars are pursuing their Ph.D. under his direct supervision. He has contributed to the areas of Computer Networks, High Voltage Engineering, Measurement and Instrumentation, Adaptive Controller, Electro-Magnetic Theory, and Intelligent Computing with his 157 publications in renowned research journals, 111 research publications in International Conferences, 73 research publications in National Conferences, more than 100 technical reports and six technical books some of which he has co-authored

E. Golden Julie received her B.E degree in Computer Science and Engg in 2005 from Anna University Chennai and ME degree in Computer Science and Engineering in 2008 from Anna University Chennai. Currently she is Pursuing her Ph.D from Anna University Chennai. Presently she is working as assistant professor in Regional centre Anna University, Tirunelveli, India She has published many research papers in various fields. Her research area includes Wireless Sensor Adhoc Networks and Image Processing. She is a member of ISTE.

S. Balaji, M.E, MISTE doing his Ph.D in Anna University, Chennai and currently working as a HOD in dept of CSE at SCAD College of engineering and Technology, Tirunelveli. His research interests are Wireless networks Mobile Computing, Network Security with apps, Wireless Sensor Networks, Cloud Computing. He has presented many papers in National and International conferences in network security, Mobile Computing, network security, and Cloud Computing. He has organized and conducted various national and international conferences, International Seminars and National Workshops. And also his methodology of teaching about TCP & UDP is hosted on Wipro Mission 10x portal. He is a life time member of ISTE.