Intelligent Management of Misbehaving Nodes In Wireless Sensor Networks

Using Blackhole and Selective Forwarding Node Detection Algorithm

Srijani Mukherjee, Koustabh Dolui
Electronics and Communications
St. Thomas' College of Engineering and Technology
Kolkata, India
{doluikoustabh, mukherjeesrijani}@gmail.com

Soumya Kanti Datta
Mobile Communication Department
EURECOM
Sophia Antipolis, France
dattas@eurecom.fr

***Abstract*—Misbehaving nodes in wireless sensor networks and ad hoc networks often disrupt the operation of the networks in more ways than one. Presence of such nodes results in congestion in paths, unreliable packet delivery and erroneous data outputs for wireless sensor networks. Existing literatures have addressed this problem using protocols with mechanisms to detect the presence of these misbehaving nodes and ignoring them altogether while delivering a packet. However, design and deployments costs are on the higher side for sensor nodes and ignoring a node entirely blocks a relay node for multiple paths passing through it resulting in inefficient use of resources. In this paper we introduce a protocol named as MMP (Misbehavior Management Protocol) to differentiate between a black hole node and a selective forwarding node. By differentiating between these two types of misbehaving nodes, paths can be chosen intelligently for the packets which might be blocked or might be allowed to pass through a node. Hence our protocol presents a misbehaving selective forwarding node as an operational node to sensors nodes whose packets are not being blocked by the node. This allows higher throughput, multiple options for selecting paths as well as more accurate data collection from the sensor nodes in wireless sensor networks.**

Keywords—Misbehaving nodes; Blackholes; Selective forwarding nodes; Wireless sensor networks

I. INTRODUCTION

Wireless Sensor Network is a network consisting of sensor nodes, equipped for collection of data from the environment as well as dissemination of the data to a remote processing/base station [1]. The raw data from the sensors are processed at the base station and corresponding actions are triggered using actuators if necessary. Wireless Sensor Networks often consist of thousands of sensor nodes, majority of which are deployed in remote locations [2]. These remote sensor nodes depend on intermediate relay nodes to communicate with the base station. If such relay nodes misbehave, data from a large group of sensor nodes are blocked resulting in erroneous outputs. The net output of a wireless sensor network is calculated as an average of the data accumulated from all the sensors. Hence if data from multiple sensor nodes are blocked, the net output is affected and accuracy is compromised. Thus, countermeasures taken against these misbehaving nodes play a major role to decide the quality of service in wireless sensor networks [3] [4]. Network level attacks on WSNs [5] include but are not limited to false routing, blackhole and sinkhole, selective forwarding nodes [6] and wormholes [7]. In this paper, we are going to construe the protocol to detect two of the network level attacks the selective forwarding nodes and the blackholes, as the behavior of these nodes attempt to compromise the performance of the network to a great extent.

A blackhole is a malicious node, which absorbs all the data received from other nodes and hence degrades the network performance and affects the net output of the sensor network [8]. A sensor selective forwarding node is more complicated than a blackhole in a way, that it blocks the packets coming from some selected sensor nodes instead of blocking all the packets as done by a blackhole. To overcome these problems with the misbehaving nodes, extensive research has resulted in publication of current literatures consisting of the proposals of a number of protocols [9]. Intrusion detection system is considered one of the worth mentioning processes to detect misbehaving nodes [10]. Another literature [11] suggests misbehaving tolerant multipath protocol which utilizes an approach enforcing cooperation from the neighboring nodes of the misbehaving node. These literatures contain efficient algorithms to ensure safe routing if the network graph remains connected after abandoning the misbehaving nodes [12]. However, these protocols have their own shortcomings, since the condition they are based on is not always feasible. The network graph may not remain connected when the number of misbehaving nodes, which have been removed from the network, is more. We have proposed a novel algorithm to ensure intelligent detection and utilization of these nodes. Our algorithm will efficiently discriminate blackholes and selective forwarding nodes specify the nodes, particularly a selective forwarding node is blocking. In that case, nodes, which find selective forwarding nodes perfectly operational, intelligently use that path containing selective forwarding node, and only the blocked nodes avoid that node. This process helps to keep paths open in a network and does not block a path for all the nodes unnecessarily when it is serving the purpose in a proper manner for a considerable number of sensor nodes.

The rest of the paper is organized as follows. In section II, we have discussed the characteristics of blackholes and selective forwarding nodes and their effects on WSNs in detail. Section III comprises of the concept of selecting multiple 'Watchdogs' for the network. In section IV, we have explained the algorithm for detecting a 'Probable Blackhole'. In section V, we have introduced the method for detection of 'Probable Selective forwarding nodes' as well as addressed all probable cases which may arise while running the detection process. In section VI, we have discussed the mechanism to declare a misbehaving node as a blackhole or a selective forwarding. Section VIII consists of the application of the discussed protocol with a relative study of other literatures. This section also summarizes the paper in a nutshell highlighting the prospects and future scope of the same.

II. Considered Attacks

The protocol, to be described in this paper is capable of detecting two network level attacks viz. blackhole attacks and selective forwarding node attacks. Fig. 1 illustrates a blackhole sensor node and a selective forwarding sensor node.

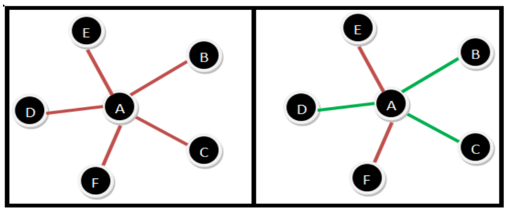

Fig. 1. A blackhole and a selective forwarding sensor node

The nodes in the figure are marked by alphabets and the paths are colored red and green. The red path signifies that the malicious node absorbs the data from those paths and does not forward the data whereas the green path signifies that the packet is subsequently forwarded along the designated path. Thus, we can deduce that the diagram on the left and right depict a blackhole and a selective forwarding node respectively. These two types of attacks are discussed in detail below.

A. Blackhole Sensor Node

As the name 'Black Hole' suggests, in this type of attack, the attacking node does not forward any packet which it receives from other sensor nodes. This packet blocking nature of the node affects the traffic flow through this node. The throughput of the neighboring nodes of the attacker is reduced drastically as the neighboring nodes cannot transmit any packet through the Blackhole [13].

The influences of a blackhole node on the network depend upon the position at which the attacker node has been deployed [14]. If the blackhole is located close to the processing/base station, it has a significant impact on the network. Since the majority of the traffic is required to go through the blackhole in order to reach the base station, the network performance is affected by a large extent. In case of such an attack, the blackhole can sever the link of the base station with other sensor nodes, attempting to disrupt the entire network. In contrast to this situation, a blackhole can cause limited harm to a network if it is located near the edge of the network, where other nodes are not bound to communicate with the blackhole in order to transmit packets to the base station. Hence the scope of a terminal black hole is limited and resultant threat to the network is diminished.

B. Selective Forwarding Sensor Node

Selective forwarding nodes exhibit characteristics which are partially different from that of a Blackhole. It acts as a blackhole for some selected nodes, i.e. it swallows the packets, which it receives from some selected nodes, but acts as a perfectly operational node for other nodes. Hence these nodes can transmit packets through the selective forwarding node treating it as a normal relay node [15]. The selective forwarding node discards packets coming from some selected nodes at its will. It is quite difficult to detect a selective forwarding node as some nodes can consider it as blackhole after failing to transmit packets through it, but at the same time, it can be considered as a reliable node by other nodes whose packets are forwarded to the correct destination by the selective forwarding node.

III. WATCHDOG SELECTION FROM NETWORK

To go ahead with the protocol, firstly we have to divide the whole network into a number of parts and assign a particular node as 'Watchdog' in each part. The watchdog will then monitor its neighboring nodes within that part of the network. Watchdogs are selected with the consideration that each node of the entire network is under the supervision of at least one watchdog. The function of the watchdog will primarily be detection of probable blackholes and selective forwarding nodes, if present among its neighboring nodes. The following algorithms are used to determine watchdogs for a particular network. If the connectivity matrix for the nodes in the entire network is specified, the algorithm to find neighboring nodes is skipped. If the connectivity matrix is not mentioned, the entire network is traversed to find the neighbors of each node using the following algorithm.

Here we define a term "status" of a node. The status of a node given by a constant S_N is used to check whether a node has been traversed to access its neighbors. Initially status for all nodes is set to 0. If at least one neighbor has been traversed once, the status S_N is changed to 1. If all the neighboring nodes have been traversed at least once, status S_N is set to 2.

A. Algorithm to Find Neighboring Nodes

- Step 1: Set status of all nodes=0
- Step 2: Start process of "Find Neighboring Nodes" by selecting any random terminal node
- Step 3: If for a node status=0, expand node to find neighbors, set status of parent node=1
- Step 4: If $S_N \neq 0$ for all neighboring nodes set status of parent node=2, else return to step 3
- Step 5: Check for the node with status=2
    - If any of its neighboring nodes has status=1, return to that node
    - Else stop the process of "Find Neighboring Nodes"
- Step 6: Generate the connectivity matrix for the network

Using the above algorithm, the entire network is traversed and the neighbors for each node are known from the process. This information is used to generate the connectivity matrix. For 'n' nodes, the connectivity matrix is an n x n matrix, each row or column corresponding to a particular node specifying its connectivity to all other nodes. Thus the i^{th} column/row of the matrix specifies the connectivity of the i^{th} node with all other nodes. If an element of the matrix A(i,j)=1, nodes i and j are connected directly and are neighbors, whereas if A(i,j)=0, the nodes are not neighbors. The connectivity between a node and itself is set to zero, i.e. A(i,i)=0. The following algorithm is used to determine the watchdogs for the network.

B. Algorithm to determine the watchdogs

- Step 1: Declare a null set w_d and node set n_k for computing watchdogs.
- Step 2: Obtain the table with each node as parent node and its corresponding neighbors.
- Step 3: Arrange the parent nodes in the order of descending neighbor count.
- Step 4: Start iteration 1 with the top of the table.
- Step 5: Add the parent node to the watchdog set w_d, add its neighbors to the set n_k If a neighbor is present beforehand in the set n_k, do not add neighbor to the set n_k.
- Step 6: Check if set n_k contains all nodes of the network. If yes stop, else select next parent node and return to step 5.

From this algorithm, we obtain the watchdog set w_d. After the end of computations for this algorithm, the nodes in this set are used as watchdogs.

C. Simulation and results

For simulation of our protocol, we have considered a sample network with 8 nodes, on which the afore-mentioned algorithms are applied. Fig. 2 depicts an illustration of the sample network. It is considered that the connectivity matrix is not specified; hence the neighboring nodes are determined first. The iterations are illustrated in Table IV.

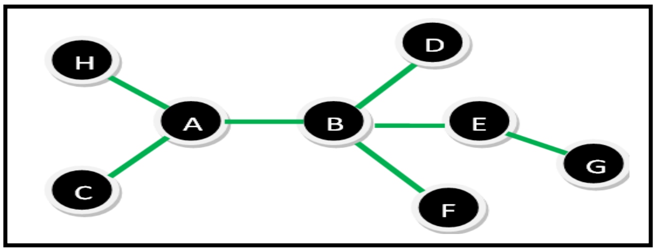

Fig. 2. A Sample 8 Node Sensor Network

From the above sample network, we select sensor node H as our terminal starting node. The status of each node is specified in subscript of the node.

TABLE I. NEIGHBORING NODES COMPUTATION

Parent node	Neighboring Nodes	Operation
H_1	A_0	By Step 3
A_1	C_0, B_0, H_1	Expand Node A
C_1	A_1	Expand Node C
C_2	A_1	By Step 4
A_1	C_2, B_0, H_1	By Step 5
B_1	A_1, D_0, E_0, F_0	Expand Node B
D_1	B_1	Expand Node D
D_2	B_1	By Step 4
B_1	A_1, D_2, E_0, F_0	By Step 5
E_1	G_0, B_1	Expand Node E
G_1	E_1	Expand Node G
G_2	E_1	By Step 4
E_1	G_2, B_1	By Step 5
E_2	G_2, B_1	By Step 4
B_1	A_1, D_2, E_2, F_0	By Step 5
F_1	B_1	Expand Node F
F_2	B_1	By Step 4
B_1	A_1, D_2, E_2, F_2	By Step 5
B_2	A_1, D_2, E_2, F_2	By Step 4
A_1	C_2, B_2, H_1	By Step 5
A_2	C_2, B_2, H_1	By Step 4
H_1	A_2	Stop, by Step 5

From the above table the connectivity matrix specified in Fig. 3 can be obtained. Each column in the matrix specifies a particular node.

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Fig. 3. The Connectivity matrix from Sample Network

From the matrix, the table V required for the computation of the watchdog nodes can be deduced.

TABLE II. NEIGHBOURHOOD NODES

Parent	Neighbors	Neighbor Count
H	A	1
A	B, C, H	3
C	A	1
B	A, D, E, F	4
D	B	1
E	B, G	2
F	B	1
G	E	1

By step 3 of the watchdog determination algorithm, the table is arranged in descending order of neighbor counts to form table VI.

TABLE III. PARENT NODES IN DESCENDING ORDER

Parent	Neighbors	Neighbor Count
B	A, D, E, F	4
A	B, C, H	3
E	B, G	2
H	A	1
C	A	1
D	B	1
F	B	1
G	E	1

The iterations for step 4 and 5 are illustrated in the following table IV. The column w_d specifies the watchdog set and the column n_k specifies the elements added to the node set. In the final iteration, B is not re-added since it is already a part of the set n_k. Since all the nodes are added to n_k in iteration 3, the process is stopped.

TABLE IV. ITERATIONS FOR WATCHDOG SELECTION

Iteration	w_d	n_k
1	B	A, D, E, F
2	B, A	A, D, E, F, B, C, H
3	B, A, E	A, D, E, F, B, C, H, G

Thus for the Fig. 2, the algorithm is applied and the sensor nodes A, B and E are selected as watchdogs. True to the objective of the algorithm, the watchdogs are selected such that at least one watchdog is assigned for each node. Using these watchdogs, the misbehaving nodes are determined.

IV. Detection of Probable Blackhole

In this section, we will address the algorithm for detection of probable blackholes within the network. In course of discussion, we will gradually introduce some nodes as ‘Probable blackholes’ in the network, which will be found blocking the watchdogs. The word ‘Probable’ signifies the probability of being a blackhole, because, we cannot consider the node as a blackhole until and unless it is found to block all the packets coming its way, which may not be the case for the node.

In this step, at a predefined interval (T_{int}), each of the watchdogs will send a particular packet to its neighbor. This interval should be chosen wisely as it would be detrimental if the algorithm is run at such a long interval that the misbehaving nodes cause harm to the network performance for a long time without being detected. Similarly, if the chosen interval is very small, the whole system will be caught up running the algorithm, detecting the misbehaving nodes and consuming a large amount of power, instead of transmitting packets. Both of these will be responsible for degrading the network performance. The packet has been termed as CHECK_PB.

This packet will have the following specifications:

- The source address and destination address fields consist of the watchdog address.
- The hop address field contains the address of the neighboring node to which the packet is being sent.

The packet is designed to be transmitted back to the source that is the watchdog itself, by which we can check if the node is working properly. The hop address is same as the neighbor’s address, so that, the packet does not reach nodes other than the watchdog and the particular neighbor. Now, the decision is taken depending on the following two conditions:

- If the watchdog receives back the CHECK_PB packet from the neighbor, it will not mark it as a ‘Probable Blackhole’ as it does not seem to swallow any packet that it is receiving.
- If the watchdog receives back the CHECK_PB packet from a particular node, it will mark the node as a ‘Probable Blackhole’, because, the node is found to block packets from the watchdogs though it may not block packets from other nodes as well.

After the decision is taken, a table is maintained by each watchdog, which records number of packets sent to the neighbor and reached back the watchdog. The following approach is used to detect probable set of blackholes.

A. Process of Probable Blackhole Determination

Let the nodes of a network be denoted by integer i ($1 \leq i \leq n$) and the watchdogs be denoted by integer k ($1 \leq k \leq N$). Each watchdog stores a table with columns specifying the value of i for its neighboring node, number of packets sent to node i denoted by Ps(i) and the total number of packets returned by node i denoted by Pr(i).

At any instant T and next instant T+1,

- Total Packets received from node i, is given by Pr(i,T) and P_r(i,T+1) respectively and so on.
- Total Packets sent to node i, is given by Ps(i,T)and P_s(i,T+1) respectively and so on.

At instant T+1, total packets in the table corresponding to node i is updated according to (1) and (2), where Pr(ins) and Ps(ins) are the number of packets received and sent in between time intervals T and (T+1).

$$P_r(i,T+1)= P_r(i,T)+ P_r(ins) \qquad \text{.1}$$

$$P_s(i,T+1)= P_s(i,T)+ P_s(ins) \qquad \text{.□}$$

At the end of every interval, the values of P_r(i,T) and P_s(i,T) are replaced by P_r(i,T+1) and P_s(i,T+1) respectively.

1) Computing probability of a node being a blackhole:

This process is carried out at an interval of one hour, from the base/processing station.

- Step 1: Repeat for i=1 to n; k=1 to N
- Step 2: Check if i is present in the watchdog table for k
- Step 3: If present, extract values of P_r(i) and P_s(i) from the table. Add the value of k to the set w_k which defines the values of k in which I is present.
- Step 4: Compute the probability of a packet returned from node i by (3) where P_r(i,k) is the total number of packets received by i from watchdog k obtained from the table of k and P_s(i,k) is the total number of packets sent to i by k.

$$\mathrm{P(i)} = {\sum_{k \in w_k} P_r(i,k)} \Big/ {\sum_{k \in w_k} P_s(i,k)} \qquad \text{.□}$$

Thus, at the end of every hour the server table updates its own table for a particular node i and its probability for returning a packet to the watchdog. Table V illustrates a sample table for a watchdog and Table VI illustrates the probability monitoring table for the base station server.

TABLE V. WATCHDOG TABLE

Node(i)	**P_s(i)**	**P_r(i)**
5	17	17
9	17	17
3	17	0
1	17	16
…	…	…

TABLE VI. PROBABILITY MONITORING TABLE

Node (i)	**P(i)**
1	0.85
2	1
3	0
4	0.71
...	…

In some cases, packets may be lost or remain undelivered but not due to presence of misbehaving nodes. This may affect the performance of reliable nodes. Hence, to prevent a reliable node from being recognized as a probable blackhole, a small constant € is defined (€>0) to compromise for the undelivered packets. If P(i)≥1-€; (€<<1) classify node as “Reliable Node”, else classify node as “Probable Blackhole”. These classified nodes are further utilized in the next section to further check for the selective forwarding nodes and blackholes.

V. Detection of Probable Selective Forwarding nodes

This section construes the third major step of the MMP protocol and is used to detect ‘Probable Selective Forwarding nodes’, which appear as Selective Forwarding nodes. This step of the protocol is carried out with the Probable Blackholes obtained from the algorithm mentioned in the previous section. As mentioned earlier, it may be discombobulating to conclude whether a misbehaving node is absorbing packets received from the watchdog only or blocking all the packets coming its way. In order to do this, a packet termed as CHECK_SF is sent by the watchdog using Strict routing option of the internet datagram. The route has to involve the most reliable node and another reliable node in such a way that:

- The most reliable node receives the packet from the watchdog and sends it to the probable blackhole.
- Another reliable node receives the packet from the probable blackhole and sends it to the watchdog.

The packet should have the following specifications:

- The source address and destination address field contain the watchdog address.
- The specified route consists of the most reliable node, the Probable blackhole and another reliable node respectively.

A. Possible Cases in Detection Process

There are two probable cases and we have entertained both of them with supporting analysis. The following discussion will shed light on the fact on how the reception of the CHECK_SF packet is used to deduce the probability of a probable blackhole being a selective forwarding node. The cases are discussed as follows:

1) Packet Returned to Watchdog

In this case, it seems that the most reliable node has received the CHECK_SF packet from the watchdog and it is most likely to send it to the Probable blackhole in the next hop. As the most reliable node has the greatest probability of transmitting a packet it is believed that it would not cause any blockage during transmission. Now, as the packet is returned to the watchdog, it can be said that the probable blackhole has transmitted the CHECK_SF packet from the most reliable node to other reliable node. From this, it can be concluded that, the probable blackhole is not a blackhole and probably is a selective forwarding node, as, the node, considered as a probable blackhole earlier has proved its reliability to other nodes, and it can be deduced that the node is blocking packets from the watchdog only.

2) Packet not Returned to Watchdog

In this case, the reliable node is not likely to block the CHECK_SF packet as it has showcased earlier traits of transmitting packets successfully. So, it may be the case, that the reliable node has transmitted the packet but the probable blackhole has blocked it, which in turn blocked the packet from returning to the watchdog. This proves that the node is blocking other nodes as well. Therefore, it can be concluded that the probability of that node being a blackhole is higher.

VI. Determination of the type of misbehaving node

Although, apparently it is concluded from the previous section, that the probability of being selective forwarding node and blackhole depends upon the reception of the CHECK_SF packet, sometimes, it may not be the case and that is why we have still considered the node as probable blackhole and not a blackhole in the second case discussed in section V. The reason behind the uncertainty is that the algorithm described so far has been found incurring a minor set of flaws. It is probable that, the detected node in the first case discussed in earlier section is a selective forwarding node, which blocks the watchdog as well as the most reliable node. So, it might not transmit any packet received from both reliable node and the watchdog. To overcome this, we have tried to find a solution to this problem, which gives a more precise result. After each interval, the watchdog table for all the watchdogs are sent to the base station. An algorithm is discussed here mathematically which collects data from the tables and detects the type of the misbehaving nodes.

A. Process to Classify BlackHole and Selective Forwarding Node

In this algorithm, the packet sending and receiving process is similar to that mentioned in the previous section. The primary difference between the two processes is that the packets are only sent to the probable black hole nodes. The packets are not sent directly to the probable black hole nodes but through reliable nodes.

Equations (1) and (2) are used to update the watchdog tables for the respective nodes. The rows containing the values of i which corresponds to a reliable node are not updated in the table and are not considered for probability computation on the base station. Equation (3) is used to update the probabilities of returning packets for the probable black hole nodes on the base station probability table. When the final values of probability are calculated for each probable black hole node, the following conditions are applied to assign the status of black hole or Selective Forwarding Node to a malicious node.

- If $\text{€}\leq P(i)\leq 1-\text{€}$; classify node as “Selective Forwarding Node”
- If $P(i)< \text{€}$, classify node as a “Black Hole”

From the probabilities obtained from the watchdog tables, the selective forwarding nodes and blackholes can be associated with the nodes that each of them are blocking. Table III illustrates a sample table stored in the base station for blocked nodes for a set of detected malicious nodes.

TABLE VII. BLOCKED PATHS FOR MISBEHAVING NODES

Node(i)	Type of Node	Blocking Nodes
4	Black Hole	i=[1,n];i≠4
7	Selective Forwarding Node	3,6,8,9
8	Selective Forwarding Node	4,1
2	Black Hole	i=[1,n];i≠2
…	…	…

VII. Related Work

Our paper illustrates the MMP protocol used to differentiate between misbehaving nodes in wireless sensor networks. The protocol facilitates intelligent selection of paths to ensure high quality of service and efficient use of available paths to optimize throughput. However, misbehaving nodes are a major aspect of research in networking with solutions ranging from competition and co-operation to queuing theory.

MAC Friendliness is a commonly used method in ad hoc networks to mitigate the effects of misbehaving nodes [16]. The impact of the behavior of the nodes on the network is analyzed using multiple variables including arrival rate, back off rate, traffic distribution and topology position. MAC Friendliness involves balancing the arrival and back off rate among nodes while the channel share of the nodes remains fixed. The back-off rate is adapted to channel condition and the requirement is balanced resulting in the same impact on the network despite having different node behaviors. Another literature [17] proposes a method for emergency users which optimizes channel utilization for each interference range and quality of service (QoS) for end to end communication. Zhefu Shi et al. [18] in an extension to literature [17] have proposed a new variable, 'channel access rate' to further improve the concept of MAC friendliness for not only heavy traffic but variable traffic load. This guarantees efficient channel utilization and removes traffic dominance by upstream nodes and unfair position of nodes. Jaramillo et al. [19] presents a mechanism using game theory to prevent false classification of nodes as selfish due to interference and packet collisions. The model used in this literature corrects the judgment of nodes based on reputation strategy and prevents punishment of wrongly deduced misbehaving nodes to optimize efficiency of the network.

VIII. CONCLUSION

The detailed algorithm for the MMP, which has been described in the previous sections, has a good prospect in the field of Wireless Sensor Networks. Intrusion Detection system [20] [21] and multipath routing have been considered to best way to prevent harm caused by misbehaving nodes so far. Many literatures have developed protocols for detecting all misbehaving nodes by only one algorithm, whereas we have addressed the fact that, a misbehaving node is not at all harmful for all the nodes within that network.

It should be considered that the cost of deployment of any sensor node is not negligible. If we abandon all the misbehaving nodes without considering it's perfectly operational behavior to some selected nodes, it will result in wastage of resources for that network and a path will be permanently blocked causing congestion in the network. Therefore, we have shed light on the process of detecting the misbehaving nodes more precisely so that it can be conducive to all nodes to know if a selective forwarding network is blocking their packets or not. This will help them, in turn, to use the selective forwarding node efficiently in order to improve network performance.

REFERENCES

[1] Y.Xu, J.Heideemann, and D.Estrin, "Energy conservation by adaptive clustering for ad-hoc networks," in *Poster session of MobiHoc'02*, 2002

[2] Ya Xu, John Heidemann, and Deborah Estrin, "Adaptive Energy-Conserving Routing for Multihop Ad Hoc Networks", Research Report527, USC/Information Sciences Institute, October, 2000.

[3] S. Khan, N. Mast, and J. Loo, "Denial of service attacks andmitigation techniques in IEEE 802.11Wireless mesh networks,"*Information*, vol. 12, pp. 1–8, 2009.

[4] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 38–43, 2004.

[5] M. Hussaini, H. Bello-Salau, A. Salami, F. Anwar, A. Abdalla, and M. Islam, "Enhanced clustering routing protocol for powerefficient gathering in wireless sensor network," *InternationalJournal of Communication Networks and Information Security*, vol. 4, pp. 18–28, 2012.

[6] Major Jose "Manny" Rivera, Jiang Li, Xiuzhen Cheng, "Attacks and Countermeasures in Sensor Networks: A Survey", Springer Network Security, 2010, pp 251-272 A. Perrig, Y-C Hu, and D. B. Johnson, "Wormhole Protection in Wireless Ad Hoc Networks," Dept. of Computer Science, Rice University, Technical Report TR01-384.

[7] A. Perrig, Y-C Hu, and D. B. Johnson, "Wormhole Protection in Wireless Ad Hoc Networks," Dept. of Computer Science, Rice University, Technical Report TR01-384.

[8] Waltenegus Dargie, Christian Poellabauer, Fundamentals of Wireless Sensor Networks: Theory and Practice, Wiley, ISBN: 0470997656, pp. 269-272.

[9] C. Ramakristanaiah, A. L. Sreenivasulu, "Identification of Misbehaving Nodes that Can Drop or Modify the Packets in Wireless Sensor Networks", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064

[10] Nabil Ali Alrajeh, S. Khan, and Bilal Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013, Article ID 167575

[11] Hanie Sedghi, MohammadReza Pakravan, MohammadReza Aref, "A Misbehavior-Tolerant Multipath Routing Protocol for Wireless Ad hoc Networks", International Journal of Research in Wireless Systems, 2012

[12] Erfan Soltanmohammadi, Mahdi Orooji, Mort Naraghi-Pour, "Decentralized Hypothesis Testing in Wireless Sensor Networks in the Presence of Misbehaving Nodes", IEEE Transactions on Information Forensics and Security, Jan. 2013, pp. 205 - 215

[13] Poonam Bisht, Arvind kumar, "Selfishness of Discriminate Node in Caching Based Wireless Sensor Network", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 2, February 2013

[14] S. Capkun and J. P. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*,vol. 24, no. 2, pp. 221–232, 2006.

[15] Issa Khalil, Saurabh Bagchi, Cristina N. Rotaru, Ness B. Shroff, "UNMASK: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks", Elsevier Science Publishers, Journal, Ad Hoc Networks, Volume 8 Issue 2, March, 2010, pp. 148-164

[16] Zhefu Shi, Cory Beard, Ken Mitchell, "Analytical models for understanding space, backoff, and flow correlation in CSMA wireless networks", Wireless Networks, April 2013, Volume 19, Issue 3, pp 393-409

[17] Zhefu Shi, Cory Beard, Ken Mitchell, "Analytical models for understanding misbehavior and MAC friendliness in CSMA networks", Elsevier, Volume 66, Issues 9–10, September 2009, pp. 469–487

[18] Dr. Zhefu Shi, Dr. Cory Beard, and Dr. Ken Mitchell, "Competition, Cooperation, and Optimization in Multi-Hop CSMA Networks with Correlated Traffic", 8th ACM Symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks, pp. 117-120

[19] Juan José Jaramillo , R. Srikant, "A Game Theory Based Reputation Mechanism to Incentivize Cooperation in Wireless Ad Hoc Networks", Journal of Ad Hoc Networks, Volume 8 Issue 4, June, 2010, pp. 416-429

[20] Abraham, C. Grosan, and C. Martin-Vide, "Evolutionarydesign of intrusion detection programs," *International Journal of Network Security*, vol. 4, no. 3, pp. 328–339, 2007.

[21] S. Northcutt and J. Novak, *Network Intrusion Detection*, SAMS,3rd edition, 2002.