Detection and Prevention of Black Hole Attack using Trusted and Secure Routing in Wireless Sensor Network

Dhananjay Bisen[1*], Bhavana Barmaiya[2], Ritu Prasad[3*], Praneet Saurabh[4*]

[1]Rajkiye Engineering College, Banda, U.P., India, PIN-210201
[2,3]Technocrats Institute of Technology Advance, Bhopal, M.P., India, PIN-462021
[4]Mody University of Science and Technology, Lakshmangarh, Rajasthan, India

bisen.it2007@gmail.com, ranu.barmaiya@gmail.com, rit7ndm@gmail.com, praneetsaurabh@gmail.com

Abstract. A wireless sensor network (WSN) is a network of devices that can communicate after gathering information by monitoring any region through wireless links. Due to this delicate arrangement several numbers of attacks directly affects the WSN functions especially denial of service (DoS). DoS is the most popular and frequent among all to affect WSN. Recently, blackhole attack has taken over it and comprises security and integrity of WSN. Secure and reliable data transmissions are the prime requirements of WSN but new evolving attacks are threats to achieve this objective. This paper proposes an algorithm that detects and recovers nodes from blackhole assaults in WSN. The proposed algorithm Trusted and Secure routing (TSR) involves detector nodes, moves in the network algorithm identifies blackhole attacks in the network, marks this node as balckhole and subsequently excludes from the network. It enables to transmit data securely with alternate path using detector node. The proposed algorithm increases the performance and the delivery ratio of data in WSN. The experimental results show reliable and secure data transmission from DoS and blackhole attacks.

Keywords: WSN, DoS, Blackhole, Security, False alarm, PDR

1 Introduction

Wireless sensor network (WSN) is a network of devices that can communicate after gathering information after monitoring any region through wireless links [1]. WSN uses sensors that senses properties like, vibration, electromagnetic strength, light, temperature, humidity and transfer the gathered data to sensor that assist pass on the data. WSN has sensing ability and communication functionalities and works in different modules [2]. Central module of WSN detects malicious node and keeps this information in a wireless sensor network. But, present malicious data injection and detection of false alarm faces pertinent issues [3]. WSN always strives to realize availability, security [2] and reliability of routing protocols. Fundamental of trust lies in locating DoS and blackhole attacks, however, gaining trust of a node is very challenging in WSN [4]. Trust, security and routing are the main challenges in WSN [5]. Data should be transmitted securely irrespective of black hole and DoS in the network [6]. This paper proposes an algorithm that detects and recovers nodes from blackhole assaults in WSN. The proposed algorithm involves detector nodes, moves in the network algorithm identifies blackhole attacks in the network, marks this node as balckhole and subsequently excludes from the network. It enables to transmit data securely with alternate path using detector node. The proposed Trusted and Secure routing (TSR) increases the performance and the delivery ratio of data in WSN. The experimental results show reliable and secure data transmission from DoS and blackhole attacks. The paper is organized as follows. Section 2 provides the related literature. Section 3 represents proposed algorithm. Section 4 provides the implementation and result analysis. Section 5 provides conclusion.

2 Related Work

Wireless sensor networks (WSN) offers connectivity through wireless link and then it collects data from various sensors deployed to achieve this task. WSN creates trust key model with a defense arrangement that utilizes grouping procedure to dynamically forward data packets [7]. **Routing in wireless network is not the same as in mobile adhoc systems [8]. WSN wireless associations are inconsistent and direction finding rules requires significant energy. Since, wireless sensors are energy deficient therefore secure and safe routing is paramount requirement of WSN. Presence of blackhole not only degrades the performance of WSN but also inflicts loss of trust in WSN [9].

Existing techniques and solutions only detects bad mounting connections and provide location and time based attacks. Various techniques for overcoming this situation have been developed and deployed. A trust distrust protocol for secure routing into wireless sensor system network is proposed that consisted of four stages. The first stage used an enhanced k-means procedure topology management, subsequent stage had test fitness estimation, next step employed fitness value grade point to mark every node and last step determined secure route for the routing according to grade point [10]. Illiano et al. [11] used available information of recommendation based trust model for the MANET and efficaciously realized the limitation in context of blackhole and location and time based attacks. The proposed algorithm will detect black hole based attacks in the network and informed to the network. Ma et al. [12] in their research pointed about a novel procedure to recognize malicious node affected by blackhole attack and also constructed dimension estimations that proved resilient to numerous compromised sensors. Subsequently, Magistretti et al. [13] performed dimension based investigations, and quantified that all the blackholes are related to measurements under unaffected environments and interrupt such connections. The drawbacks of the scheme are that the dimensions encompass and duplicate information. Son et al. [14] provided information about routing security in their method and detected blackhole attacks. Li et al. [15] in their work illustrated that like MANET, hosts in WSN are particularly defenseless to all attacks. Route discovery and creation are based nohe same mechanism of sending

RREQ packet to the all the neighboring node for path but malicious node reply for RREQ complicates the routing. This whole process actually makes WSN vulnerable to new attacks and packet routed through them causing high packet drop ratio. In recent times some researchers explored this domain though various bio inspired techniques [16] that have successfully attained different objectives this domain [17, 18, 19]. The proposed Trusted and Secure routing (TSR) is designed to detect black hole based attacks in the network and then inform the network.

3 Proposed Method

This section presents the Trusted and Secure routing (TSR) to overcome the problem of blackholes in WSN.

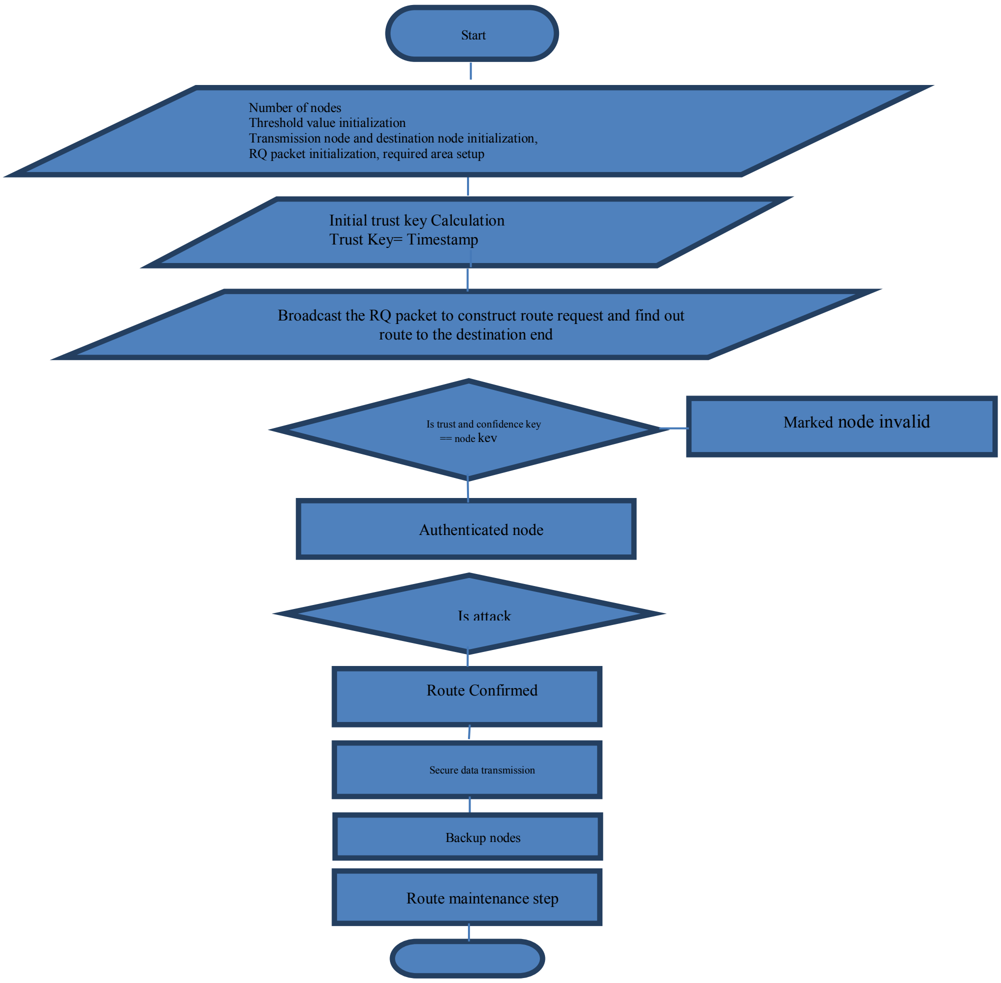
Start
Number of nodes
Threshold value initialization
Transmission node and destination node initialization,
RQ packet initialization, required area setup
Initial trust key Calculation
Trust Key= Timestamp
Broadcast the RQ packet to construct route request and find out route to the destination end
Is trust and confidence key == node kev
Marked node invalid
Authenticated node
Is attack
Route Confirmed
Secure data transmission
Backup nodes
Route maintenance step

Figure. 1. Flow Diagram of proposed algorithm

Above fig. 1 represents the flow diagram that represents all the initialization parameters of the algorithm. The rectangle represents all the processing of the algorithm. The decision box represents all the conditions of the proposed Trusted and Secure routing (TSR). Initially all the required parameters are provided input to the input as algorithm. The parameters are source node, number of nodes, destination node etc. All the threshold values are provided to the algorithm.

```
Step 1: Start
Step 2:  Fill mandatory information in RQ packet of sender. Broadcast the RQ packet to construct route
request and find out route to the destination end.
Step 3: The request is acknowledged by intermediary node or destination node .
                If RQ received is identical then
                                Throw away the RQ
                Else if fresh or restructured route is established then
                                Next update the routing information entry for the source node
                                Build or update inverse route in the direction of the source node
                End if
Step 4: If receiving node is one or the other the intermediary or target node with newer route then
                     Goto step 2
               Else
                     Take the mandatory field values as of the received RQ
                     Update compulsory fields in the RQ beforehand broadcasting
                     Rebroadcast the RQ packet
              End if
Step 5:  If sending node is target node then
                     Increase the destination series number
             End if
                    Fill RP packet with the mandatory columns
           Send the RP packet on the inverse route in the direction of the source
Step 6: By means of an intermediate node on the inverse route or the source node.
                   Record the mandatory column values from the received RP
                  Attachment of the corresponding documented values into RP
                  If the neighbor directing RP is striking as blacklisted then
                        Throw away the RP
             Else if
                        Fresh and restructured route is found then
                 Update the transmitting table record for the destination node
         End if
                If receiving node is the main source node then
                       Reject the RP
                Direct the data through the forward direction if the route is newer and the subsequent hop is
reliable
         Else
                Forward the RP packet on the inverse route in the direction of the source node
         End if
Step 7: Update trust
               For neighbor information entry do
                     Authenticate the presence of attack information form neighbor
                     Estimate trust value of the neighbor node
            If the neighbor follows attack information then
                     Identify the node as mistrusted node
            Else if the neighbor doesn't have information of attack value, and
                     suggested as trusted node then Identify the node as trusted node
             End if
         End for
               For routing information entry do
                    Discover the information of the subsequent hop from the neighbor information
            If the subsequent hop is found to be disbelieved in the neighbor information then
            Start a local route finding process to find out an alternative route to the destination
        End if
    End for
Step 8: Belief recommendation
            Create the vacant blacklist for reference purpose
                For each neighbor information entry do
            If the neighbor is identified as disbelieved node then
                Supplement the neighbor identity into the blacklist
          End if
      End for
Step 9: Integrate the blacklist into the HELLO data packet
         And broadcast the HELLO data packet as of the neighbors
             Take HELLO data packet from the neighbor
        If the neighbor directing the HELLO data packet is trusted then
             Take the blacklist from the HELLO data packet
        For each information in the blacklist do
             Discover the equivalent information in the neighbor route table
        If the neighbor information occurs then
               Set reference value as disbelieved for the neighbor
          End if
    End for.
Step 10: End
```

Initially all the mandatory information is filled in the request packet (RQ) of the source node. The request packet (RQ) is then broadcasted to construct route request and search route to the destination. The request is acknowledged by intermediary node or destination node. If received request is identical then simply throw away the RQ. If received request is fresh or restructured route is established then next update the routing information entry for the source node and build or update inverse route in the direction of the source node. The next step is to check the information for receiving node. If receiving node is one or the other the intermediary or target node with newer route then again all the mandatory information is filled in the request packet RQ of the source node otherwise take the mandatory field values as of the received RQ update compulsory fields in the RQ beforehand broadcasting and again rebroadcast the RQ packet. Next step is to check if sending node is target node. If sending node is target node then increase the destination series number. After that, it fills reply (RP) packet with the mandatory columns and unicast the RP packet on the inverse route in the direction of the source. Intermediate node or the source node record the mandatory column values from the received RP and attachment of the corresponding documented values into RP. If the neighbor directing RP is striking as blacklisted then throw away the RP otherwise if fresh and restructured route is found then update the transmitting table record for the destination node.

If receiving node is the main source node then reject the RP direct, data through the forward direction if the route is newer and the subsequent hop is reliable else forward the RP packet on the inverse route in the direction of the source node. The next step is to update trust. For each neighbor information entry authenticate the presence of attack information form neighbor. Estimate trust value of the neighbor node if the neighbor follows attack information then identify the node as mistrusted node. Else if the neighbor doesn't have information of attack value, and suggested as trusted node then identify the node as trusted node. For routing information entry do the following steps repeatedly discover the information of the subsequent hop from the neighbor information if the subsequent hop is found to be disbelieved in the neighbor information then start a local route finding process to identify an optional path for desired output. Next step is belief recommendation in proposed algorithm. Create the vacant blacklist for reference purpose for each neighbor information entry do the subsequent step if the neighbor is identified as disbelieved node then supplement the neighbor identity into the blacklist. Next step is to integrate the blacklist into the hello data packet and broadcast the hello data packet as of the neighbors take hello data packet from the neighbor. If the neighbor directing the HELLO data packet is trusted then take the blacklist from the hello data packet for each information in the blacklist do the following step and discover the equivalent information in the neighbor route table if the neighbor information occurs then set reference value as disbelieved for the neighbor. Trusted and Secure routing (TSR) also increases performance and the ratio of data delivery in network. The experimental outcomes show the system is good for safe data transmission secure from DoS and blackhole attacks.

4 Result Analysis

This section presents the experimental setup and experimental results carried to measure the performance of Trusted and Secure routing (TSR) and its comparison with current state of the art (AODV).

Table 1 Simulation parameters

Parameter	Value
MAC layer Protocol	802.11
Traiffc Type	CBR-UDP
Routhing protocol	AOMDV
Initial Energy	1 Joule
Number of Nodes	50
Packet Size	1024 s/ sec
Frequency Range	1025 GHz
Received Power	0.01 watts
Trainsmitted Power	0.02 watts
Simulation area	1500 x 1500
Mobility model	Random way point
Maximum mobility	5m/sec to 25m/sec
Percentage of malicious nodes	0% to 50%
Simulation time	200 to 1000 sec
Number of connections	10
Communication range	250m
Channel bandwidth	2 Mbps

Table 1 presents the performance parameters used for implementation like, dimension, total nodes, traffic, transmission rate, routing protocol, transmission range, sensitivity, transmission power etc. Below are detailed performance parameters on which results are obtained and analyzed.

(i) Simulation area: The simulation area represents the region where simulation is performed. Different simulation areas are used for implementation, like 500X500, 850X1200.

(ii) Simulation duration: The overall time elapsed in complete execution of simulation is called simulation duration. Simulation is 100s for experiments.

(iii) Average Delay: This metric depicts the freshness of data containers. It is well-defined as the average epoch between the twinkling an information packet is directed by an info source besides the instant the sink accepts the data container.

(iv) No of mobile nodes: The nodes used in simulations are 30, 50 with mobility and without mobility.

(v) Transmission range: The distance at which the information can be communicated precisely is termed as transmission range. Transmission range is 250m in simulation.

(vi) Data Delivery Ratio (R): This metric designates both the damage ratio of the path and routing technique and the energy mandatory to get data packets. This denotes the ratio between the amounts of information containers that are sent by the source and same desired by the sink.

(vii) Movement model: Random waypoint model is used for simulation.

(viii) Traffic type: The traffic type indicates types of traffic used by simulation environment. We have used CBR traffic type for implementation.

(ix) Max node speed: Maximum node speed as 5ms to 30s used in simulation.

(x) Rate packet per size: 2 packets per size are used for implementation.

(xi) Data payload: Different amount of data payload is used in implementation. In experiments 28 to 512 bytes data pay load is used.

(xii) Protocol: Protocol represents set of rules for data communication. AODV protocol is used for implementation.

(xiii) Neighbor discovery probability: The discovery of the neighbor for data transmission.

(xiv) Neighbor discovery latency: The latency of the node during neighbor discovery.

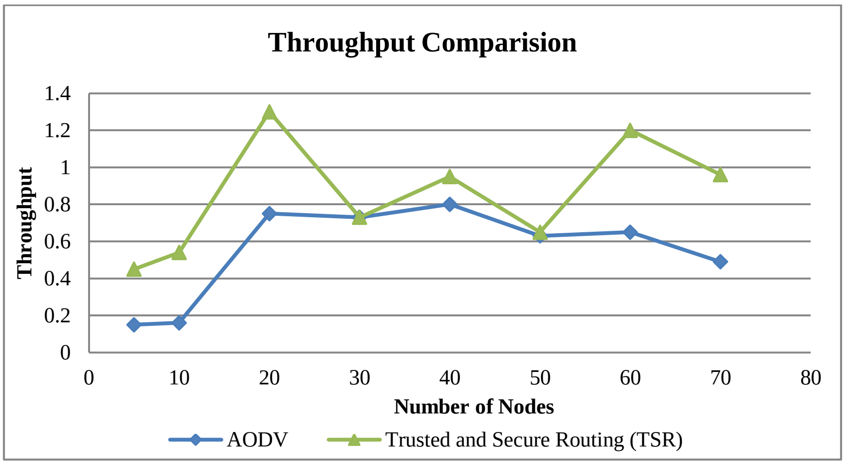

Fig. 2 Throughput analysis

Above fig. 2 represents throughput analysis of attacks and security arrangement with an increase in number of nodes in the networks. Attackers aim is to drop the data packets or to hold the resources for that the communication is affected. Overall in existing work the throughput is maximum and security is minimum while in proposed work the throughput is minimum with maximum security.

Black hole and security scheme's Packet Delivery Ratio performance is depicted in fig. 3 with an increase in number of nodes in the networks. In WSN, when blackhole is introduced in the network data packets are dropped as a consequence that leads decrease in the percentage ratio of data. Newly introduced detector nodes in WSN identify blackholes attack in the network. The identified node is then blacklisted from the network and they are excluded from network so that a different secure path established to complete the transmission.

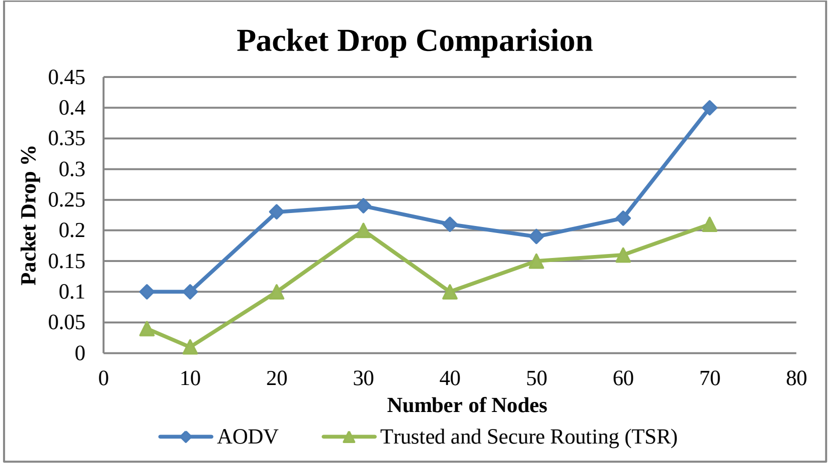

Fig. 3 PDR analysis

Before hand, ratio of packet drop was maximum and after using detector node ratio of packet drops becomes minimum.

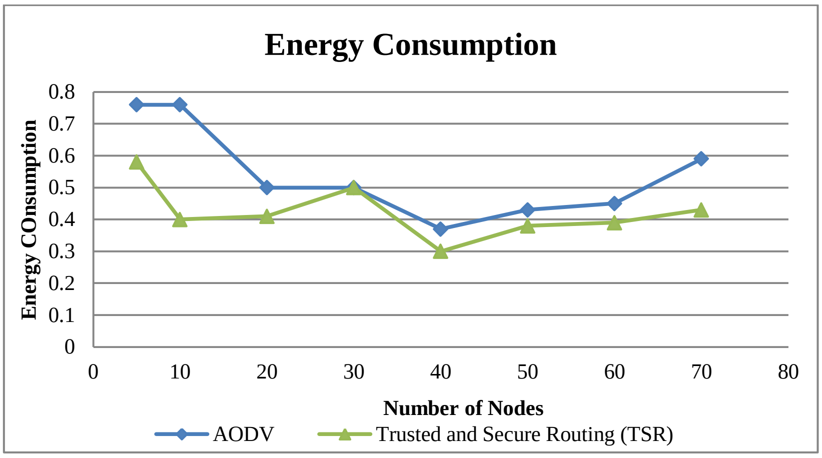

Fig. 4 Energy conversion analysis

As represented in fig. 4 energy consumption of ActiveTrust is more in the existing method as compared to the energy consumption of the proposed method. Precisely, energy consumption is reduced as compared to ActiveTrust. Figure 4 very clearly states that the proposed method required lesser energy as compared to the existing method with an increase in number of nodes in the networks.

5 Conclusions

In WSN, transmission of data can be achieved if no malicious node remains present in the network. In situations with presence of malicious nodes and false alarm, WSN finds it very difficult to continue transmission. Data packets need to be transmitted securely irrespective of blackhole attack or malicious information in WSN. This paper introduced an innovative technique that protects network from blackhole and DoS attack by identifying the attack in WSN. The proposed system automatically detected the compromised node and then authenticated the secure path to achieve communication. The proposed method also prevented the network from blackhole attack and established trust through blacklisting the attacked node and making route safe. The experimental results demonstrated that proposed method outperformed the existing methods and enhanced energy proficiency in WSN.

References

1. Cao, Q., Abdelzaher, T. , Stankovic, J. , Whitehouse, K., Luo, L.: Declarative tracepoints: A programmable and application independent debugging system for wireless sensor networks. In: Proc. ACM SenSys, Raleigh, NC, USA, pp. 85–98, (2008).
2. Shu, T., Krunz, M., Liu, S.: Secure data collection in wireless sensor networks using randomized dispersive routes. In: IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, (2010).

3. Souihli, O., Frikha, M., Hamouda, B., M.: Load-balancing in MANET shortest-path routing protocols.In: Ad Hoc Netw., vol. 7, no. 2,pp. 431–442, (2009).
4. Khan, S., Prasad, R., Saurabh, P., Verma, B.: Weight Based Secure Approach for Identifying Selfishness Behavior of Node in MANET, Advances in Intelligent Systems and Computing, vol 701. Springer, pp 387-397, (2017).
5. Aad, I., Hubaux, J.-P., Knightly, W., E.: Impact of denial of service attacks on ad hoc networks. In: IEEE-ACM Trans. Netw., vol. 16, no. 4, pp. 791–802, Aug. (2008).
6. Mandala, S., Jenni, K., Ngadi, A., Kamat, M., Coulibaly, Y.: Quantifying the severity of blackhole attack in wireless mobile adhoc networks. In: Security in Computing and Communications. Berlin, Germany: Springer, pp. 57–67,(2014).
7. Liu,Y., Dong,M., Ota,K., Liu, A.: ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks. In: IEEE Transactions on Information Forensics And Security, Vol. 11, No. 9, pp. 2013-2028, (2016).
8. Dong, M., Ota, K., Liu, A., Guo, M.: Joint optimization of lifetime and transport delay under reliability constraint wireless sensor networks. In: IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 1, pp. 225–236, Jan. (2016).
9. Liu, X., Dong, M., Ota, K., Hung, P., Liu, A.: Service pricing decision in cyber-physical systems: Insights from game theory. In: IEEE Trans.Services Compute. vol. 9, no. 2, pp. 186–198, Mar./Apr. (2016).
10. Dong, W., Liu, Y., He, Y., Zhu, T., Chen, C.: Measurement and analysis on the packet delivery performance in a large-scale sensor network. In: IEEE/ACM Trans. Netw., vol. 22, no. 6, pp. 1952–1963, Dec. (2014).
11. Illiano, P., V., Lupu,C. E.: Detecting Malicious Data Injections in Event Detection Wireless Sensor Networks.In: IEEE Transactions On Network And Service Management, Vol. 12, No. 3, pp-496-512, September (2015),
12. Ma, Q., Liu, K., Zhu, T., Gong, W., Liu, Y.: BOND: Exploring hidden bottleneck nodes in large-scale wireless sensor networks. In: Proc. IEEE ICDCS, Madrid, Spain, pp. 399–408, (2014).
13. Magistretti, E., Gurewitz, O., Knightly, E.: Inferring and mitigating a link's hindering transmissions in managed 802.11 wireless networks. In: Proc. ACM MobiCom, Chicago, IL, USA, pp. 305–316, (2010).
14. Son, D., Krishnamachari, B., Heidemann, J.: Experimental analysis of concurrent packet transmissions in low-power wireless networks. In: Proc. ACM SenSys, San Diego, CA, USA, pp. 237–250, (2005)
15. Li, X., Ma, Q., Cao, Z., Liu, K., Liu, Y.: Enhancing visibility of network performance in large-scale sensor networks. In: Proc. IEEE ICDCS, Madrid, Spain, pp. 409–418, (2014).
16. Saurabh,P., Verma,B.: An Efficient Proactive Artificial Immune System based Anomaly Detection and Prevention System, Expert Systems With Applications, Elsevier, 60, pp 311–320, (2016).
17. Saurabh,P.,Verma,B., Immunity inspired Cooperative Agent based Security System, The International Arab Journal of Information Technology, Vol. 15, No. 2, pp.289-29, (2018).
18. Saurabh,P.,Verma,B, Sharma,S.: An Immunity Inspired Anomaly Detection System: A General Framework, In Proceedings of Seventh International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA 2012), vol 202 of the series Advances in Intelligent Systems and Computing, Springer, pp 417-428, (2012).
19. Saurabh,P.,Verma,B, Sharma,S.: Biologically Inspired Computer Security System: The Way Ahead, Recent Trends in Computer Networks & Distributed Systems Security, CCIS, Springer, vol 335,pp 474-484, (2011).