Effectual Approach for Blackhole assault avoidance using Soft Computing

[1]Rupinder Singh, [2]Rajneesh Randhawa
[1]Research Scholar, [2] Assistant Professor
[1,2]Department of Computer Science, Punjabi University, Patiala
Email: [1]lavy.sidhu00@gmail.com, [2]drrajneeshrandhawa@gmail.com

ABSTRACT

Wireless networks are susceptible and inclined to grouped assaults at various layers from numerous sources and in this manner it is required to comprehend the component and in addition scientific categorization of assaults. By this point of view, there is have to research the network level assaults, their effect and medicinal measures with the goal that the general situation can be made secured. The nodes in wireless condition are influenced unfavorably by number of assaults centering of the assets utilized by the nodes partaking in the correspondence. These network nodes are for the most part connected with the grouped utilitarian angles including battery or vitality, control, log of neighboring nodes, reserve and number of administrations. In a network assault, the pernicious node or packet endeavors to briefly or for all time stop these parameters so that the bona fide and reasonable correspondence can be harmed. Various algorithmic arrangements conflict with grouped assaults yet there is tremendous extent of research in this section. This composition underlines the assaults on wireless networks with their related measurements so the strong calculation can be created for general security and respectability. The proposed approach is incorporating insect province advancement as nature enlivened approach by which the packets misfortune can be exceptionally lessened. The close-by nodes filling in as ants assumes control over the packets and hand over towards the legitimate goal by which the general correspondence is made secured and uprightness mindful. The proposed approach is useful and enhanced towards over 25% on the assessment of grouped parameters.

Keywords: Wireless Sensor Network, Reliable Communication, Wicked Wireless Node Attacks, Wireless Sensor Network Security.

INTRODUCTION

In wireless networks, there are portable nodes which are associated with each other utilizing radio or related transmission line with no physical foundation. Wireless Network alludes to a particular situation having versatile nodes associated by means of portable switches, base stations or satellites utilizing which the general network can be controlled and observed. There are number of utilizations in which wireless sensor networks are coordinated. In traditional way, the wireless networks are actualized for the simplicity of versatility, remote openness and cross locale availability.

TAXONOMY OF WIRELESS TECHNOLOGY NETWORKS

- Wireless LAN
- Wireless WAN
- Wireless Mesh Network
- Wireless PAN
- Wireless MAN
- Cellular Network
- Global Area Network
- Space Network

FEATURES OF WIRELESS NETWORKS

- Autonomous
- Dynamic and Effective Load Balancing
- Scalability
- Network Access Control
- Distributed, Arbitrary and Connected Operations
- Multihop based Routing
- Network Topology in Dynamic
- Network Scalability
- Light Weight Terminals
- Ease and Speed of deployment
- Decreasing dependency on infrastructure
- Mobility and Quality of Service
- Portability

Table 1: Comparison between WSN and Mobile Ad Hoc Networks

WIRELESS SENSOR NETWORKS	MOBILE AD HOC NETWORKS
Energy Consumption more and generally non rechargeable due to remote and sensitive locations	Energy is not the issue because of recharging
Very far and not accessible physically in general	More close of Human Experts / Users
Data Aggregation / Grouping	No need of aggregation
Clustering	Each mobile node act as router itself
Security and Integrity are the key issues	Security is not an issue as it is always very close to human user

IEEE 802.11 STANDARDS

IEEE 802.11 refers to a set of specifications devised by IEEE for the representation of Wireless LAN (WLAN) technology. The standard 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. IEEE accepted this standard in year 1997.

The key threats to Wireless Technologies are hereby summarized

- Interception or Eavesdropping
- Wormhole or False Gateway Attack
- Non Optimal Path or Byzantine Allocation Attack
- Jamming
- Blackhole attack
- Byzantine attack
- Rushing attack

BLACK HOLE ATTACK

Packet Drops Attack or traditionally the blackhole attack is one of precarious assault in wireless communication which leads to higher packets loss because of intruding nodes. This research work focus on the development and implementation of a novel and effective algorithm for achieving the security and avoidance of blackhole in the wireless networks.

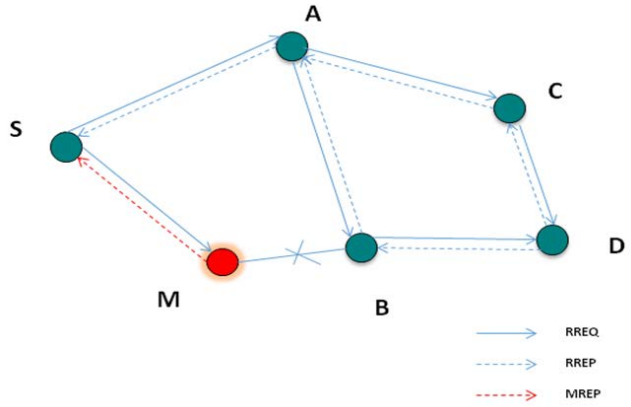


Figure 1: Black hole attack

REVIEW OF LITERATURE

There are a few difficulties posture by the asset constraints in the remote sensor arranges because of the vulnerabilities that may happen because of element conduct of systems. For deep and empirical analysis of the security and integrity aspects in wireless networks, a number of research papers are analyzed from various sources. Following are the approaches and conclusions of research papers and manuscripts.

[1] In this paper, a novel and effective approach for the energy encryption is addressed. The approach is associated with WPT (Wireless Power Transfer) for improving the overall performance of the network in terms of security and integrity. The proposed approach is uses dynamic, secured and authorization based energy consumption so that the overall performance of network can be enhanced.

[2] In this research manuscript, an effective and high performance approach for security in clustered wireless environment is proposed. This approach used is query process based paradigm to implement the security in wireless networks. Using the proposed approach in this paper, the security and integrity is preserved on multiple parameters against various attacks

[3] In this paper, the authors address the use and integration cryptographic hash approaches for implementation of security and authentication in wireless networks. This work underlines and implements MD5 (Message Digest) and SHA (Secured Hash Algorithm) as a hybrid algorithm to ensure and enhance the security in wireless networks

[4] In this work, the lightweight cryptography is implemented for security and privacy issues in the wireless networks. A unique and effective ultra lightweight approach KLEIN to improve the overall efficiency of the network environment is proposed and implemented.

[5] Homomorphic Encryption is the base issue taken in this work. In this paper, the authors implemented symmetric encryption and homomorphic encryption for performance evaluation. Finally, it is found and concluded that the performance cannot be highly improved using homomorphic encryption approaches

[6] In this paper, the authors propose a lightweight hash, Neeva-hash fulfilling the especially critical considered lightweight cryptography. Neeva-hash depends on upon wipe method for cycle with programming liberal change which gives excellent ability and required security in RFID progression. The proposed hash can be utilized for some application based purposes.

[7] The work in this paper addresses the issues of WSN requests and lightweight security. This paper addresses and devises a new approach for security and integrity in the wireless networks.

[8] This work considers two applications: “hop by hop transmission of information from cluster nodes to the base station and direct communication to clustered nodes information by mobile clients by strategy for mobile gadgets. Because of the hardware blocks of WSNs, some irrelevant effort operations, for occurrence, symmetric cryptographic approaches and hash functions points are utilized to finish a dynamic key association. The session

key can be redesigned to keep dangers of assault from every correspondence. With these strategies, the information accumulated in wireless sensor networks can be all the more safely gave. Additionally, the proposed plan is dejected down and separated and related game plans". In addition, a NS2 era is made in which the exploratory results demonstrate that the designed correspondence convention is workable.

[9] In this paper, the issue of key management is addressed for security and integrity in the wireless environment. The key goal of this research manuscript is to evaluate, compare and extract the suitable and high performance protocol for the wireless scenarios.

[10] To address the objectives of security and respectability, this paper proposes a lightweight module considering the robust operations. The proposed cryptographic game plan utilizes elliptic turn focuses to attest the going on focus focuses and as one of the puzzled helper parameters to make the pseudorandom bit movement. This social occasion is utilized as a bit of XOR, change and creamer operations with a specific completed target to encode the information pieces. The trial results in light of Mica2 sensor bit display that the proposed encryption game plan is nine times complex than the LED custom and two times speedier than the TWINE convention. The authors have also performed distinctive certain tests and cryptanalytic assaults to study the security way of the calculation and found the figure provably secure.

NATURE INSPIRED APPROACH BASED BLACKHOLE AVOIDANCE

The projected approach for blackhole avoidance is having ant colony optimization in which there are number of wireless mobile nodes which communicate with each other in association of multiple nodes for secured transmission.

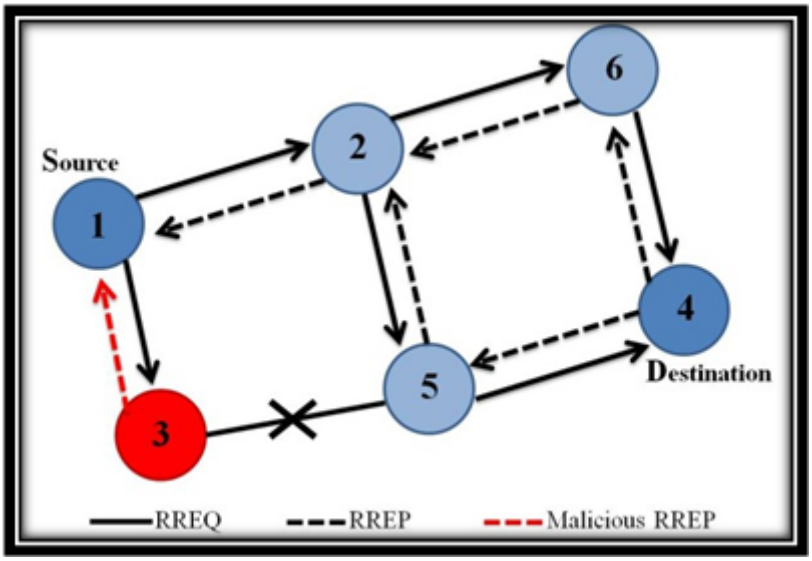


Figure 2: Black hole attack

The Classical Approach is making use of Cryptography which is not highly secured

- The cryptography functions can be sniffed and exploited by third party applications
- In the proposed work, the concept of Server Agent (SA) is introduced which keeps track of the location and registration id
- SA checks the suspicious location and earlier registration status and only then the communication will take place

- Any new node willing to communicate in the network will have to log to SA so that the identity cannot be forged by the Sybil Node
- The Sybil Nodes using this approach are repelled back and logged to the server for appropriate signature matching

BLACKHOLE AVOIDANCE MECHANISM

In this classical RSS Based Approach (RBA) technique, followed RSS (Received Signal Strength), so if any nodes with RSS greater than the given threshold will be considered as the attacker as per the traditional work. This approach is totally not applicable for the wireless networks because mobile nodes may have various signal strength.

In order to prevent this attack a centralized approach is needed that will monitor the mobile nodes.

Step 1 : Allocation of the Wireless Networks with Unique Id and Authentication with the Centralized Server so that any attempt of Blackhole can be recognized.
Step 2 : Route Request and Node Recognition with the Server
Step 3 : Verification of the Source Node and Identification of Route Reply from Authenticated Nodes. The Server Agent initiates the process of registration and logging of valid nodes.
Step 4 : Broadcasting of Route Reply in association with the Server Agent so that any attempt of cracking cannot move ahead and the network can be made secured
Step 5 : Identification and Selection of the adjacent node having more power and energy so that the persistent and secured connection can take place
Step 6 : The Ant Colony Optimization based nature inspired approach is integrated and each node is functioning as ant in the wireless scenario
Step 7 : The ants in the mobile wireless communication keeps track of the transmission and if packet drops, the hand-over shift takes place
Step 8 : Using proposed approach the packets will be lost at very negligible level due to higher and global optimization that is achieved by the ant colony optimization.

TOOLS AND TECHNOLOGIES USED

- Linux : Ubuntu 16.04 LTS 64 Bit
- ns2
- xgraph
- GNU Plot
- awk

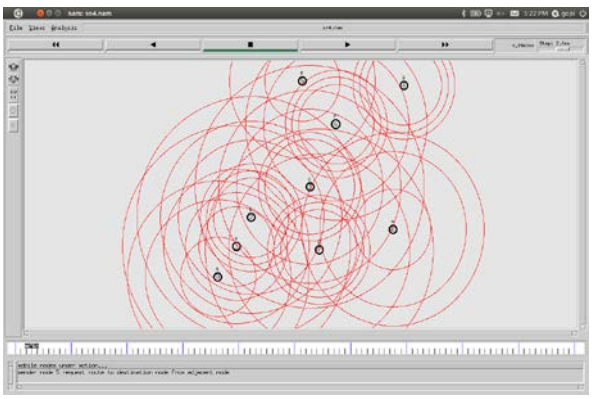


Figure 3: Mobile Nodes in Motion and Transmitting Signals

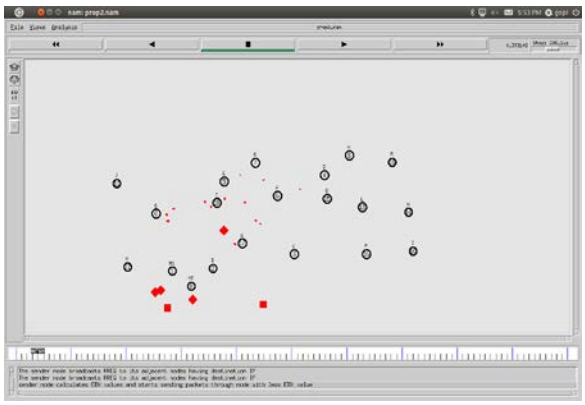


Figure 4: Route Request (RREQ)

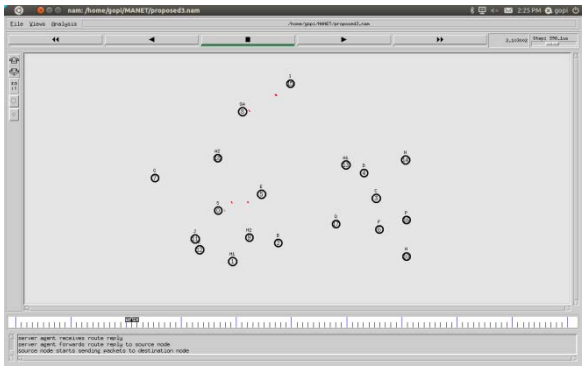


Figure 5: Route Reply (RREP)

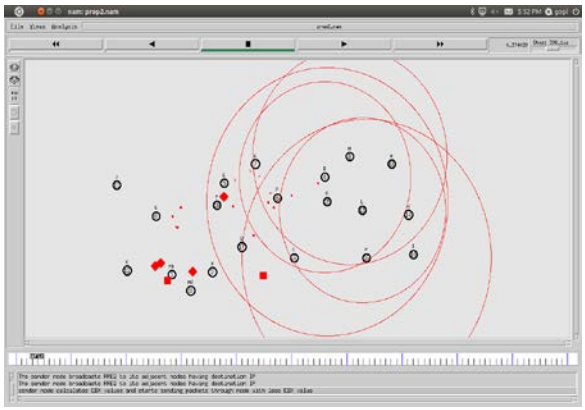


Figure 6: Packets Transfer in the Wireless Nodes

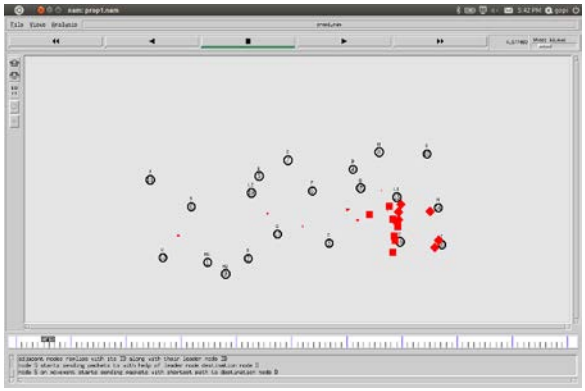


Figure 7: Representation of Packet Drops

Packet Transfer Rate

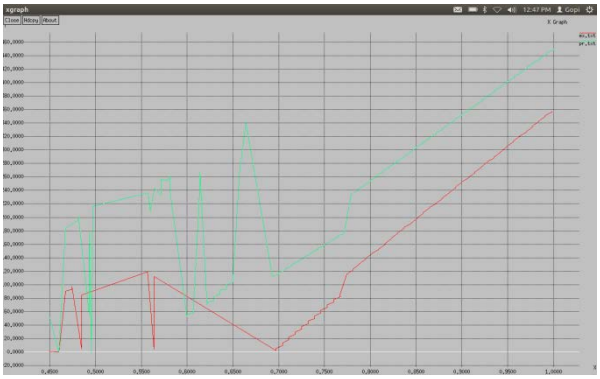


Figure 8: Evaluation of Packets Transfer

Packets Loss

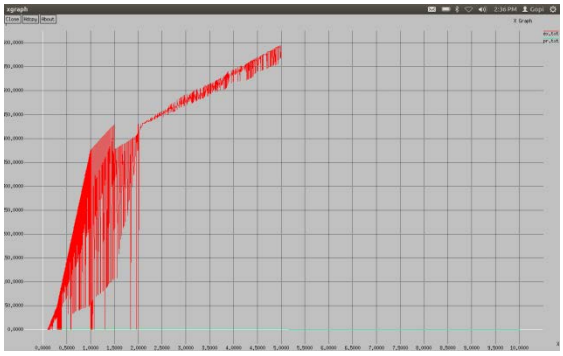


Figure 9: Packets Loss

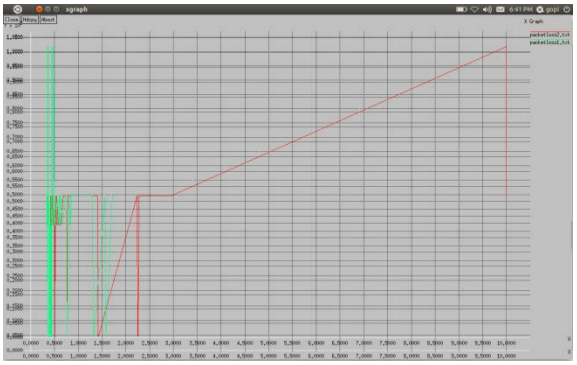


Figure 10: Comparison of Packets Loss

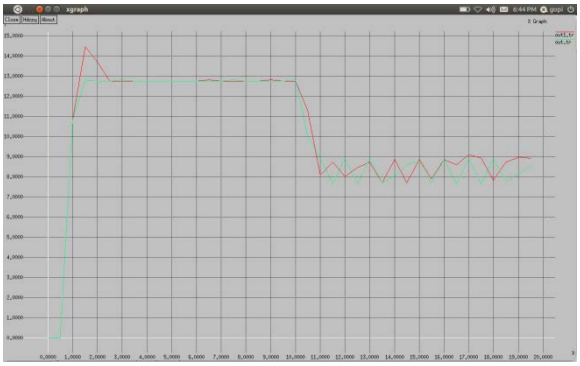
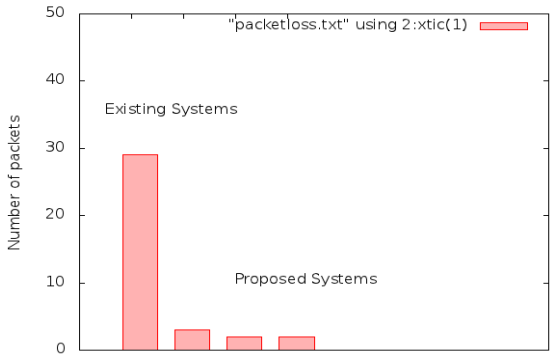


Figure 11: Evaluation of Jitter

Table 2: Packets Loss

Greedy Based Traditional Approach	**Nature Inspired Approach based Blackhole Avoidance**
300	101
390	189
389	168
490	190



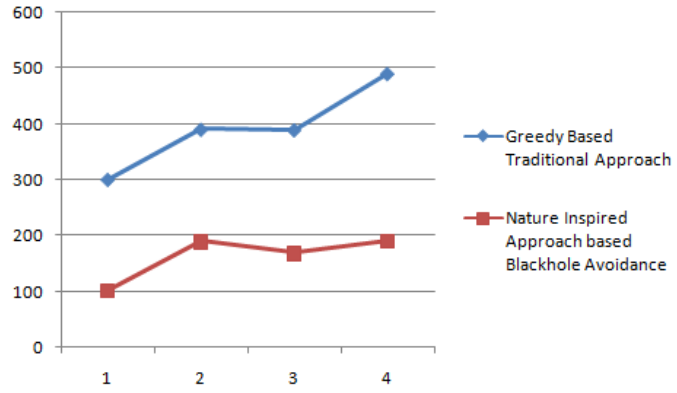


Figure 12: Analysis of Packets Loss after Trace File Analysis

Table 3: Throughput - Transfer Rate

Greedy Based Traditional Approach	**Nature Inspired Approach based Blackhole Avoidance**
60	98
68	80
89	94
64	90

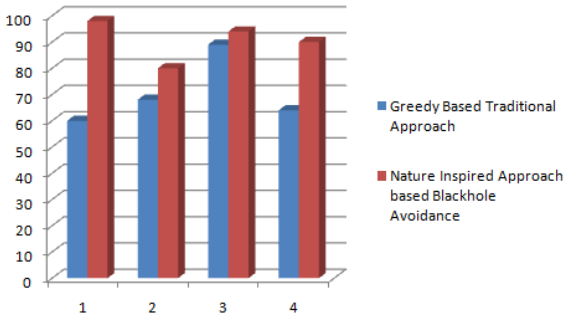


Figure 13: Analysis of Transfer Rate after Trace File Analysis

Table 5: Complexity

Greedy Based Traditional Approach	**Nature Inspired Approach based Blackhole Avoidance**
90	26
80	42
86	40
98	30

Table 6: Overall Performance

Greedy Based Traditional Approach	Nature Inspired Approach based Blackhole Avoidance
60	87
78	89
53	96
50	98

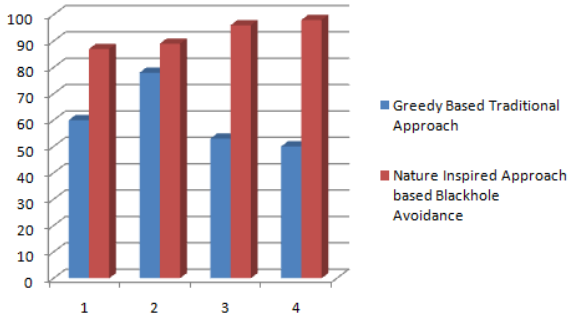


Figure 14: Analysis of Packets Loss after Trace File Analysis

It is evident from the results that the proposed ant colony based nature inspired approach is giving better and effectual results in terms of less packets loss and higher degree of throughput. The phase of jitter evaluation is effectual and better in the proposed approach which denotes the overall performance and escalated efficiency.

CONCLUSION AND SCOPE OF FUTURE WORK

There are number of algorithms and approaches for encryption and dynamic cryptography for security in wireless networks. Still, there is need to propose, devise and implement the salt based hybrid and dynamic cryptography so that the higher level of security and integrity can be proposed. The networks should be secured with the design of a new algorithm using hybrid cryptography approach for security in the wireless base control station.

The current security approaches can be made hybrid and high performance using metaheuristic approaches including Ant Colony Optimization, Simulated Annealing, Honeybee Algorithm, Firefly Algorithm, River Formation Dynamics and many others.

REFERENCES

[1] Aydos, M., Sunar, B., & Koc, C. K. (1998). An elliptic curve cryptography based authentication and key agreement protocol for wireless communication. 2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications Symposium on Information Theory.

[2] Biswas, K., Muthukkumarasamy, V. and Singh, K., 2015. An Encryption Scheme Using Chaotic Map and Genetic Operations for Wireless Sensor Networks. Sensors Journal, IEEE, 15(5), pp.2801-2809.

[3] Bussi, K., Dey, D., Kumar, M. and Dass, B.K., 2016. Neeva: A Lightweight Hash Function.

[4] Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004

[5] Chen, C.L., Chen, C.C. and Li, D.K., 2015. Mobile Device Based Dynamic Key Management Protocols for Wireless Sensor Networks. Journal of Sensors, 2015.

[6] Cochavy, Baruch, Method of efficiently sending packets onto a network by eliminating an interrupt, US Patent Issued on August 18, 1998
[7] Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, A Security, Privacy and Trust Architecture for Wireless Sensor Networks, 50th International Symposium ELMAR-2008, 10-12 September 2008, Zadar, Croatia
[8] Donna Andert, Robin Wakefield, and Joel Weise, Professional Services Security Practice, Sun BluePrints™ OnLine - December 2002, Trust Modeling for Security Architecture Development
[9] Ghosal, A. and DasBit, S., 2015. A lightweight security scheme for query processing in clustered wireless sensor networks. Computers & Electrical Engineering, 41, pp.240-255.
[10] Kiruthika, B., Ezhilarasie, R. and Umamakeswari, A., 2015. Implementation of the Modified RC4 Algorithm for Wireless Networks. Indian Journal of Science and Technology, 8(S9), pp.198-206.
[11] Phaneendra, H. D., & Smitha, B. C. (2017). Enhanced BRM Technique to Avoid Blackhole Attacks on MANETs. International Journal of Engineering Science, 10873.
[12] Chowdari, R., & Srinivas, K. (2017). A survey on detection of Blackhole and Grayhole attacks in Mobile Ad-hoc Networks.
[13] SINGH, O., SINGH, J., & SINGH, R. (2017). MRWDP: Multipoint Relays Based Watch Dog Monitoring And Prevention For Blackhole Attack In Mobile Adhoc Networks. Journal of Theoretical & Applied Information Technology, 95(6).
[14] Panos, C., Ntantogian, C., Malliaros, S., & Xenakis, C. (2017). Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks. Computer Networks, 113, 94-110.
[15] Kaur, H., & Mangat, K. (2017). Black Hole Attack in Mobile ad Hoc Networks: A Review.