International Journal of Engineering & Technology, 7 (3) (2018) 1299-1303

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i3.12485
Research paper

An energy efficient flexible delay tolerant network with adaptive secured framework (ASF-DTN)

Dhanabal S [1], Dr.Amudhavalli P [2], Dr. Prasanna Venkatesan G. K. D [3]

[1] *Research Scholar, CSE, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India*
[2] *Research Supervisor, CSE, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India*
[3] *Professor & Dean(Research & Development),SNS College of Engineering, Coimbatore, Tamil Nadu, India*
**Corresponding author E-mail:* nkldhanapal@gmail.com

Abstract

Delay tolerant networks are widely used in mobile communications because of network withstanding capability of delay. However, when the connectivity of nodes increases, data loss may occur while transmission. Due to the malicious behavior of nodes the data may get permanently lost, which is known as black hole attacks and there is a chance to partial data loss because of the lower energy level of a node, which is known as a gray hole attack. In existing work, the data capacity of a node is not limited, so most of the highly energy efficient node contains a huge amount of data, when compared to other nodes which may lead to random attack. To overcome this, we propose a subjective capability model (SCM) for each and every node to limit the capacity of each node. ASF-DTN prevents collision attack and injection attack by implementing Kalman filtering, which can statistically analyze the behavior of nodes while each and every transmission. Here, we propose an effective node optimization scheme using genetic algorithm with a fitness function to find out energy efficient nodes among the optimal path for effective communication and its performance.

Keywords: *ASF-DTN; Black-Hole; Collusion Attack; Gray Hole Attack; Kalman Filtering; Node Optimization; Subjective Capability; Wireless Sensor Networks*

1. Introduction

A Delay tolerant network is a collection of nodes, but most of all the characteristics of each node are different due to the energy level, distance and circumstances [1]. The DTN networks are widely used due to its outstanding performance. Delay tolerant networks are vulnerable to malicious attacks such as collision attack or data injecting attack, black hole attack and gray hole attack [2]. Due to the malicious behaviors of node, the network architecture may misbehave [3]. There arises a lack of communication between the nodes in DTN architecture due the following reasons [4].

1) Attacks or malicious behavior of nodes
2) Non Optimized Data path

Here we describe the brief explanation about both two scenarios

2. Attacks or malicious behaviors of node

Due to the black hole attacks [5] the entire data packets that have been transferred from source node to destination node gets dropped. [6] It may happen due to the hackers or due to the lower energy level of the sensor nodes. Likewise, gray hole [7], [8] attacks occur due to either the malicious activity or else by poor state of the node. Data collision or data injection attacks are widely discussed now days. It is a scenario in which the malicious user can inject data into the encrypted content. This happens, when a hacker can't find out or decrypt the content. When the data is injected into the encrypted data, mostly it becomes to be unrecoverable. It becomes very complicated to recover the original data that has been routed from the destination.

3. Non optimized data path

When the data is forwarded to the destination in a longer path or else via the shortest path, which contains non energy efficient nodes, then it may lead to delay and when the path size is increased, the transmission efficiency will degrade i.e. ($p\alpha \frac{1}{r}$). Let the number of paths (p) is increased then the transmission rate (r) will decrease. Both are inversely proportional and here NE denotes non-energy efficient node. Equation illustrates below illustrates this scenario.

$$r = n/ (p1/n+p2/n+p3/n)\text{-}NE \quad (1)$$

Where transmission efficiency depends on the probability of connected node in a network and the energy efficiency of a new node.

4. Related work

Various methodologies are proposed to provide a flexible routing mechanism even in the presence of various kinds of attacks. But there were some limitations and drawbacks. ASF-DTN proposed by considering all the issues in our existing work. In this section we present some existing schemes along with their limitations

Li and Das developed a trust management scheme [13] which monitors the forwarding behavior of a node to its next node and that are all updated frequently for the reliable transmission but it can't withstand against black hole and gray hole attack. Li et al. [14] developed an encounter model to detect a black hole attack in delay tol-

erant networks, but it's not applicable for large scale DTM's. Encounter record maintenance is not scalable, it is vulnerable to injection attacks.

Li's developed a mitigating routing scheme [15] in which a node's behavior is always monitored by a contact node. Contact node is responsible for the overall functionality of a network. If a node transmits a data to another node, then the data forwarding node sends the acknowledgment to the contact node and the receiver node also sends an acknowledgment to the contact node. Acknowledgment contains received packet information, forwarded path information and the route information to the destination. If the packet size doesn't match with the source content, then it will raise an alert to the contact node, then contact node sends the data in alternate path. But it does not propose to solve node optimization issues.

Tie que and aoyang proposed a scheme called ROSE that works based on node degree and angle sum calculations for classifying highly energy efficient node among DTN network nodes. So that, the source can pass the data to the destination rather than passing via all possible paths. It provides a security against various attacks with the help of node authentication scheme. The nodes are formed into a cluster by its radius level. But this method does not provide security against black hole and gray hole attacks and it is not suitable for energy efficient node optimization.

Probabilistic anomaly detection [16] was proposed by Gao, Zhu, Xiao, Du and Lu which provide trust based authentication services based on the contact information and the transmission history of each node. Its authentication providing scheme, is a kind of probabilistic approach because it provides authentication based on connection probability between the new node to node clusters. The works [17], [18], [19] utilizes the centralized encounter record in which a transmission history is updated in the routing table for each and every transmission .But there may be a chance to modify the encounter table illegally. ASF-DTN is proposed by considering all the issues in the existing system, and the performance of ASF-DTN is compared with its related existing works that is discussed in section V.

5. Proposed work

To overcome the issues here we propose ASF-DTN framework which provides subjective capability, i.e. each node should consume or contain the subjective amount of data to overcome the random attacks. This framework also consists of ASF-KF (Kalman filtering) which can statistically analyze the data transmission history (TH) of each node for every transmission. ASF-DTN is flexible to monitor the optimized energy efficient node by implementing GA-FF (Genetic Algorithm with Fitness Function).

5.1. Subjective capability model (SCM)

The Subjective capability framework that we are proposing in ASF-DTN can withstand against random attacks as well as malicious attacks. In random attacks, nodes are attacked by a random manner rather than the subjective attack i.e. malicious attack. [9], [10].

To achieve the energy efficient network architecture, the radius of sensor nodes should be wide to get connected with 60% of the nodes in a delay tolerant network. To satisfy the above condition, SCM model clusters the network into partitions, where each cluster connects with all other clusters. Unlike our existing methodologies, our proposed framework will enhance the energy efficiency of delay tolerant networks.

SCM model limits the energy consumption of each node to avoid malicious node that may consume high energy when compared to all other nodes. When a node wants to join in a cluster it should have some high energy efficient node nearby. It should also capable of perceiving all the information of its neighborhood node. Assume node 1 is a highly energy efficient and node n is the newly requested node to join in a nearby node cluster. The equation illustrated below defines the connection probability of new nodes in a network.

$$\text{CP}(N_n) = \text{CP}(N_{n1}) - D_n \quad \sum_{n=1}^{N} D_n \tag{2}$$

Where, CP represents the connection probability of a new node,CP (Nn1) represents the connection probability of node n1 with other nodes and Dn represents the distance value from node 1 to the new node.

Algorithm: SCM
Input: No of nodes N,Node cluster,Radius r
Procedure: DTNbuild ()
For all t € T_n
If time T_n is not expired with r
Calculate deg (m) $CP\ (N_{n1}) - D_m$
If node degree (m, <Min thresh (m) & &CP (m) ≈1) then
Cluster m into c
For d=1 to n
Broadcast (d -> c)
Else
Ignore m
End for
End if
End procedure

Adaptive SCM

Proposed SCM is an adaptive framework, if the value of connection probability decreases (CP) or distance value increases, then the authorized node removes the inefficient node from its network partitioned cluster.

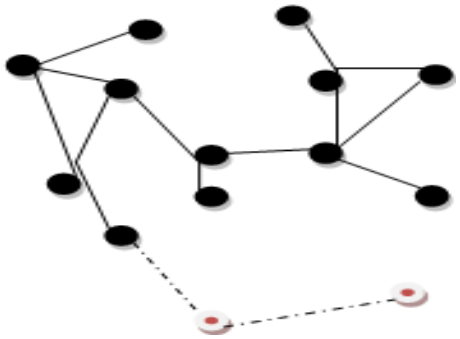

Fig. 1: SCM Model.

High energy efficient node
Less energy efficient node

Adaptive SC Algorithm
CP (m) ≈1) then
Step 2: For d= [1] to n
Step 3: Cluster m into step 4: Broadcast (d -> c)
Else
For d=1 to n
Remove m from c

Where each connection requires the degree of existing node and connection probability of a new node with its neighborhood node partitioned cluster. Thresh (m) is fixed based on the DTN level of architecture. When CP (m) ≈1 or CP (m)>0.7 then, it provides better node link connectivity and it provides efficient transmission. For each transmission, connection probability and node degree are calculated and the architecture of DTN is further optimized using genetic algorithm. Where, m represents the connection probability of a new node. If m does not satisfy the condition it will be considered as non energy efficient node and it will be removed by node cluster itself. So our proposed ASF-DTN adaptively partitions and clusters each and every node in a delay tolerant network based on node degree and connection probability. Then the each partitioned cluster is grouped inside DTN. The performance of ASF-DTN is efficient, when compared to our existing works because ASF-DTN is the cluster of each partitioned cluster.

5.2. ASF-KF against data injection

ASF-KF (Kalman filtering) is a kind of filtering approach that statistically analyzes the data transmission history (TH) of each node during every transmission. Data injection is a scenario in which the malicious user can inject data into the encrypted content. This happens when a hacker or decryption key of the content can't be found, and then he/she may try to inject some data into the transmitted content. When the data is injected into the encrypted data, mostly it can't be unrecoverable. It will be very complicated to recover the original data that has been routed from the destination.

The cryptography mechanisms and the keys are sensitive and it can provide the security for data, but sometimes it fails to recover the original content of the transmitted message when the data injection occurs. Each and every transmission history (TH) of a node in a statistically calculated by the ASF-KF i.e., transmission history is being monitored by the ASF-KF model in our architecture.

Let us consider the node 1 transmits the packets to node 4 as illustrated in figure 2, then the data is transmitted via node1-node2, node 2-node3 and node3-node4 or else via node1-node7, node7-node6, node6-node5, and node5-node 4. Then, the TH of each transmission of each node is statistically computed with the help of Kalman filtering, i.e., received packet information of node1, forwarded packet information, available paths from node 1 and received packet information of node 2 and the available paths from node 2 and forwarded packets from node 2–node3. The calculation is computed for all transmissions and the misbehavior node can be detected with the help of statistical analysis record

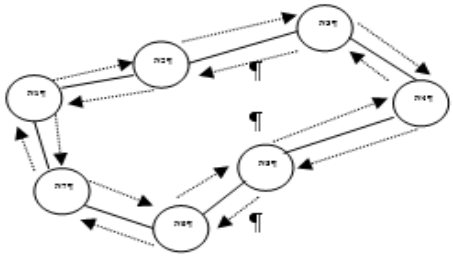

Fig. 2: Dtn Architecture**.**

The architecture illustrated above represents the route details of DTN networks. The probability of data injection Prb(I) is calculated based on the transmission history of N1-N2, N3-N4, N4-N5 etc. The packets that have been transferred and received (I) can be denoted by the equation illustrated below.

$$\text{Prb (I)} = \frac{D[P(FN1) - P(RN2)]}{P(FN1)} * 100 \quad (3)$$

Where P (FN1) denotes the data packets forwarded to node 1, D (RN2) denote the received data packet details, P (I) denotes the probability of injecting.

Algorithm:Kalman Filtering Pseudo code
Input: maxthres,v
Output:Prb(I)
Procedure: kalmonfilter ()
Step 1: For all TH
Step 2: Find D
Step 3: P (I) =D/D (FN1)*100;
Step 4: If (P (I)>maxthres) then
Block the path;
Rise alert to source
Step 5: Else
Broadcast d
End for
End if

Where V = maximum threshold of injection D=Differentiated value of data transmission rate. In this architecture path N7-N6 is malicious node, i.e., when node 7 transmits the data packets to node 6 the packets are dropped, Unlike our existing approaches [14], [15], [16], the proposed ASF-KF leads to block the further transmission paths in DTN architecture. If a transmission founded to be a leakage, it raises alert to the source and it identifies an alternate path based on adaptive SCM node construction methodology, which is discussed in 3.1 so our proposed ASF-KF can effectively calculate the statistical analysis to each transmission. So, false data injection can be effectively eliminated. We will discuss the path optimization function in part 3.4.

5.3. ASF-KF against black whole and gray whole attack

Our proposed ASF model also consists ASF-IF (Iterative Filtering) along with ASF-KF, which can effectively identify the malicious node in Delay Tolerant Networks. Malicious nodes leads to data loss or it rises to delay in a communication network, hence it degrades the quality of DTN. ASF-IF provides the service quality and it provides integrity proof. There are two types of common major attacks

1) Black hole attack
2) Gray hole attack

Due to the black hole attacks the entire data packets that have been transferred from source node to destination node gets dropped. It may happen due to the hackers or due to the lower energy level of the sensor nodes. Likewise, gray hole attacks occur due to either the malicious activity or else the poor state of the node.

Standalone ASF-KF can classify the malicious node among benign nodes. It classifies the malicious node based on the TH value of each transmission. An efficient transmission's differentiated value D should be 0, i.e., D (FN1)-D (RN2)=0.

If differentiated value D (FN1)-D (RN2) is varies than a predefined value, then the attack is termed as a gray whole attack. If the differentiated value D (FN1)-D (RN2) is approximately equal to D (FN1) then it is termed as a black hole attack. (Predefined value is nothing but DTN-IF notifies each node about the data transmission details such as packet information that are all forwarded in a source and neighborhood node details, the data received by its previous node.)

ALGORITHM: Iterative Filtering Algorithm
Input D, weight vector of nodes w
I←0
W←
Repeat
Calculate T^{i+1}
Calculate W^{i+1}
I←i+1
Until trustable network constructed

Where T represents a trustworthiness of a clustered network inside a DTN, where the T is measured based on the distance vector value of each node. The trustworthiness of a DTN architecture depends on the node degree, distance between each node inside a partitioned cluster. The loop is manipulated for each and every transmission cycle until it convergence an energy efficient partitioned node.

Each node in a partitioned cluster sends the acknowledgement to its master node (authenticated/authority node). ACK consists of the data forwarded from its previous node and the data received by itself. Master node can accurately detect the malicious node in a network cluster by comparing the predefined value and the acknowledgement details.

5.4. GA-FF (genetic algorithm with fitness function)

ASF-DTN architecture consists of GA-FF for node optimization. It optimizes the node after the results, i.e., any intrusions have raised in a node cluster then, it eliminates the malicious node and it generates a new optimized path.

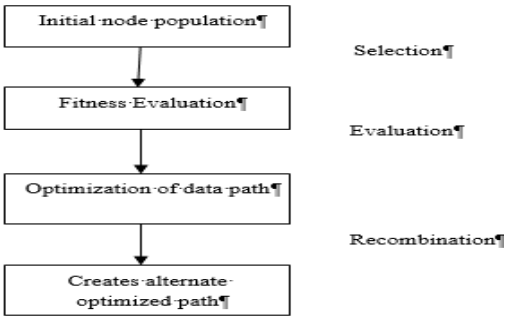

Fig. 3: GA-FF Node Optimization

In existing work [11], [12], pass the data to the destination, the available paths are found by the optimization technique such as, Ant colony based optimization, Dijkstra's shortest path finding approach etc. But there were no further optimization proposed after detecting intrusion. So the data will be passed to the entire available path due to the exigency.

Our proposed GA-FF in ASF can flexibly identify the energy efficient node among the nodes cluster and it finds the optimal nodes. The following steps denotes the node optimization scheme of our proposed ASF architecture.

6. Architecture of ASF-DTN

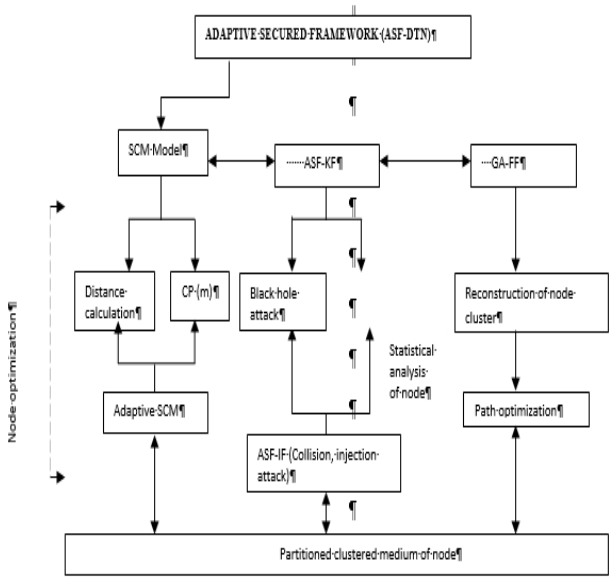

Fig. 4: ASF-DTN Architecture.

6.1. Node initialization-optimization

In node optimization phase, the source and destination node are fixed based on the requirements. Then ASF-SCM identifies the optimal, highly-energy efficient paths among the multi-route DTN. It eliminates the less energy efficient paths adaptively without requiring any approval from source node and it updates the route information in the route table. A node can be joined into a network if it satisfies the specified condition of SCM model. A node should have the required connection probability and it should be closer to the network, to join in a partitioned cluster.

Step 1: Initialization of destination
Step 2: Cluster formulation i.e. C1 (n1, n3, n6, n7, n9), C2 (n10, n11, n13).
Step 3: D calculation to avoid the black hole and gray hole attack.
Step 4: P (I) Calculation to detect injection attacks, collision attacks.
Step 5: Evaluation of highly energy efficient path.
Step 6: Updating route information.
Step 7: Pass the data to destination.

6.2. Secured node authentication mechanism

ASF-DTN consists security based certificate issuing scheme in which a newly joined node should perceive credentials to participate in a partitioned cluster node.

creq
Cer1 creq
Cer N

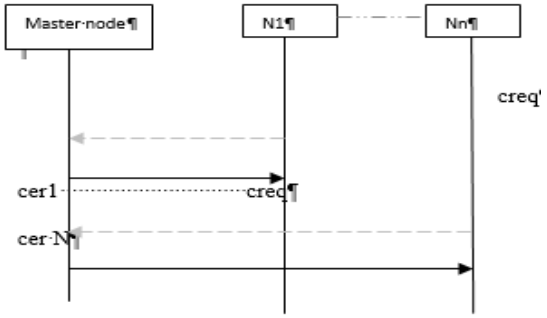

Fig. 5: ASF-DTN Security Based Authentication Mechanism.

Where, creq represents a connection request of a new node, and master node issues certificates based on the node credentials.

An idle node, which is high-energy efficient, considered as a master node. It verifies the certificate of each node while data transmission. So node injection attack can be avoided with the help of this scheme.

6.3. ASF-DTN against various attacks

The main module of the proposed architecture is ASF-KF, which can statistically analyze the TH of the each transmission in DTN architecture. By the mathematical analysis of TH, black and grey hole attacks can be identified.

ASF architecture includes iterative algorithm which is used to effectively identify the collision and injection attacks, which are all discussed in earlier section-II.

6.4. Genetic algorithm with fitness function

It initializes the routing table, which is all updated with SCM model and it generates all possible highly energy efficient optimal paths based on the fitness probability of each node. Hence the less energy efficient nodes are all further filtered by GA-FF. The ASF-GA_FF algorithm is illustrated below, where RR represents routing table.

Algorithm: ASF-GA_FF
Input SCM-RT
Process: GA_FF
Step 1: Generate P //optimal path based on fitness
Step 2: Computecross_over
Step 3: Compute mutation
Step 4: Update SCM-RT

7. Performance analysis of ASF-DTN

The performance of ASF-DTN is analyzed by comparing node optimization strategy, security implementation mechanism and transmission efficiency of our existing trending methodologies such as ROSE, mitigating routing and encounter record based approaches while comparing, we can observe that ASF-DTN's performance of node optimization is high when compared to ROSE's node optimization technique because of the implementation of genetic algorithms with fitness function.

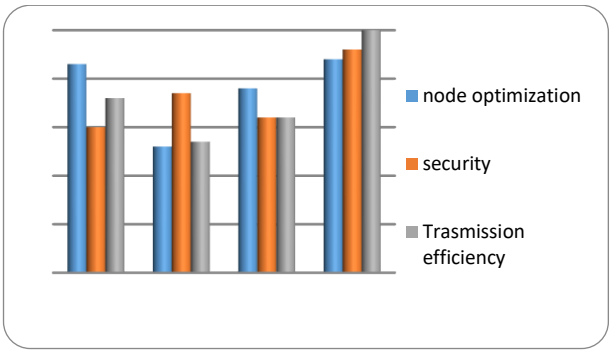

Fig. 6: Performance Analysis of ASF-DTN.

Figure 6 clearly represents the comparison strategy for security is high to mitigating routing technique, but our ASF-DTN method provides a better security service than the mitigating routing technique. The ASF-DTN's transmission efficiency is really higher than other techniques. A Genetic algorithm with fitness function is providing better node optimization, through the ASF-DTN to us.

8. Conclusion and scope for future work

Delay tolerant networks are applicable for the networks, which have to adapt a delay. However, when the connectivity of nodes in DTN increases, then it leads to data loss. Owing to the malicious activity of a node in DTN, it is vulnerable to attacks such as black holes, collision attack injection attack and grey whole attack. Unlike our existing work, ASF-DTN proposed a subjective capability approach, which makes a threshold amount of all nodes to have passed a certain amount of data to avoid random attacks. ASF-DTN provided the secured transmission against collision attack and injection attack by implementing Kalman filtering and iterative filtering, which can statistically analyze the behavior of nodes while each and every transmission .The implemented genetic algorithm with fitness function evaluated the highly energy efficient optimal node in a DTN and the performance was compared with existing approaches. In our future work we will work to identify the behavioral changes of each node with digital signature based authentication mechanism.

References

[1] Sarawagya Singh, Elayaraja.K," a survey of misbehaviors of node and routing attack in delay tolerant network" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 2, February 2015.

[2] PreetiNagrath, SandhyaAneja, G.N.PurohiInformation Networking (ICOIN), 2015 International Conference on" Defending Flooding Attack in Delay Tolerant Networks"published in IEEE.

[3] Alberto Lopez Toledo, Josep M. Pujol, Pablo Rodriguez," Fair Routing in Delay Tolerant Networks" published in infocom 2009, ieee.

[4] Atul Sharma,, Dr. Dinesh Singh ,Poonam Sharma, Dr. SanjeevDhawan, "Selfish Nodes Detection in Delay Tolerant Networks "2015 1st International Conference on Futuristic trend in Computational Analysis and Knowledge Management (ABLAZE-2015).

[5] Aysha Al Hinai, Haibo Zhang and Yawen Chen,"Mitigating Blackhole Attacks in Delay Tolerant Networks"2012 13th International Conference on Parallel and Distributed Computing, Applications and Technologies,".

[6] SriramBharaniS Ms. Savitha Saranya , Tissin "Detecting and Eliminating Grey Hole Attack in Delay Tolerant Network", Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-12, 2016 ISSN: 2454-1362, http://www.onlinejournal.in.

[7] ErmanAyday,Hanseung Lee, FaramarzFekri" Trust Management and Adversary Detection for Delay Tolerant Networks".

[8] Rupali Sharma" Gray-hole Attack in Mobile Ad-hoc Networks: A Survey" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3) 2016, 1457-1460.

[9] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley,"Robustness of interdependent networks under targeted attack,"Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.,vol. 83, no. 6,p. 065101(R), 2011.

[10] R. H. Li, J. X. Yu, X. Huang, H. Cheng, and Z. Shang, "Measuring robustness of complex networks under MVC attack," in Proc. 21st ACM Int. Conf. Inf. Knowl. Manage. , New York, NY, USA, Oct. /Nov. 2012, pp. 1512–1516.

[11] Marco Dorigo and Gianni Di Caro "Ant Algorithms for Discrete Optimization".

[12] S. Sivakumar, Dr. C.Chandrasekar "Modified Dijkstra's Shortest Path Algorithm" Vol. 2, Issue 11, November 2014.

[13] N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks,"Elsevier J. Ad Hoc Netw., vol. 14, pp. 1497–1509, 2013 https://doi.org/10.1016/j.adhoc.2011.01.018.

[14] F. Li, J. Wu, and A. Srinivasan,, Thwarting blackhole attacks in disrupt-tolerant networks using encounter tickets," in Proc. INFOCOMM 2009, pp. 2428–2436.

[15] Tie Qiu, Senior, AoyangZhao,Student,Xia,Weisheng Si,Dapeng Oliver Wu," ROSE: Robustness Strategy for Scale-Free Wireless Sensor Networks"2017,IEEE Transactions on ACM/networking.

[16] Z. Gao, H. Zhu, S. Du, C. Xiao, and R. Lu, "PMDS: A probabilistic-misbehavior detection scheme toward efficient trust establishment in Delay-tolerant networks,"IEEE Trans. Parallel Distrib.Syst., vol. 25, no. 1, pp. 22–32, Jan. 2014 https://doi.org/10.1109/TPDS.2013.36.

[17] Thi Ngoc Diep Pham and Chai Kiat Yeo "Detecting Colluding Blackhole and GreyholeAttacks in Delay Tolerant Networks,"IEEE Transactions on mobile computing,may-2016.

[18] KarthikeyanBhargavan, GaetanLeurent "Transcript Collision Attacks:Breaking authentication in TLS, IKE, and SSH"NDSS '16, 21-24 February 2016.

[19] S.Bhargavi&Vishnu Prasad Goranthala, "The Impact of Collusion Attacks in WSN withSecure Data Aggregation System" International Journal of ResearchVolume 2, Issue 08, August-2015.

[20] Kalaivanan M. and K. Vengatesan.: Recommendation system based on statistical analysis of ranking from user. International Conferenceon Information Communication and Embedded Systems (ICICES), pp.479-484, IEEE, (2013).

[21] J.W. Ho, M. Wright, and S.K. Das, "Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing", IEEE Transaction on Mobile Computing, June 2011.