International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org || PP. 01-10

Analyzing And Replacing The Selfish Node Using Fa-Rep Protocol in Manet

*K.Yazhini[1], Dr. D. Loganathan[2]
[1,2(]*Dept. of Computer Science and Engineering, Pondicherry Engineering College, Puducherry,India)*

Abstract : *We propose neighbor coverage based false alarm method for detecting selfish node in MANET. The false alarm will be differentiated from other techniques. If any alarm generated means we should verify the reason of the alarm. If the number of nodes exceeds the threshold value means it will get confirm as selfishness alarm else the alarm has been raised because of the network disconnections. So we propose node replacement algorithm which provide a more security to the mobile network. An active node is set up, which is nearly adjacent to the source node. The selfish node will be replaced by the active node when alert of selfish node produced. Hence it is an effective technique to detect selfish node and get replaced the selfish node by active node. This technique provides more security in MANETs.*

Keywords: *Ad hoc networks, capacity, mobility, Manet's, selfish node's***.**

I. Introduction

1.1 AD-HOC networks

In computer networking, an Ad-hoc network which does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed wireless networks. As simple as Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other.

1.2 Mobile computing

Mobile computing is a technology that allows transmission of data, via a computer, without having to be connected to a fixed physical link. Mobile voice communication is widely established throughout the world and has had a very rapid increase in the number of subscribers to the various cellular networks over the last few years.An extension of this technology is the ability to send and receive data across these cellular networks. This is the principle of mobile computing. Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution to the biggest problem of business people on the move - mobility.Mobile adhoc network is a self-configuring infra-structure less network of mobile devices connected by wireless. Each device in a MANET is free to move Independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.MANETs are a kind of wireless Ad-hoc networks that can change locations and configure itself on the fly. Because MANETS are mobile, the use wireless connection to connect to various networks. This can be standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers),while others may be connected to the Internet. For example, A VANET is a type of MANET that allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the vehicles' to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets.A stateless protocol is a communication protocol that treats each request as an independent transaction that is unrelated to any previous request that the communication consists of independent pairs of requests and responses. A stateless protocol does not require the server to retain session information or status about each communication partner for the duration of multiple requests.Mobile Ad-hoc network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas other needs the aid of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of any infrastructure. This property makes these networks highly exible and robust.

The earliest MANETs were called "packet radio" networks, and were sponsored by DARPA in the early 1970s. BBN Technologies and SRI International designed, built, and experimented with these earliest systems. Experimenters included Jerry Burchfiel, Robert Kahn, and Ray Tomlinson of later TENEX, Internet

and email fame. It is interesting to notethat these early packet radio systems predated the Internetand indeed were part of the motivation of the original Internet Protocol suite.Later DARPA experiments included the Survivable Radio Network (SURAN) project, which took place in the 1980s. Another third wave of academic activity started in the mid 1990s with the advent of inexpensive 802.11 radio cards for personal computer. Current MANETs are designed primary for military utility; examples include JTRS and NTDR.The popular IEEE 802.11 ("Wi-Fi") wireless protocol incorporates an ad-hoc networking system when no wireless access points are present, although it would be considered a very low grade ad-hoc protocol by specialists in the field. The IEEE 802.11 system only handles traffic within a local "cloud" of wireless devices. Each node transmits and receives data, but does not route anything between the network's systems. However, higher-level protocols can be used to aggregate various IEEE ad-hoc networks into MANETs.Generally, the communication terminals have a mobility nature which makes the topology increases the challenges of the design of Ad-hoc networks. Each radio terminal could be divided generally into three parts, power consumption for data processing inside the RT, power consumption to transmit its own information to the destination, and finally the power consumption when the RT is used as a router, i.e. forwarding the information to another RT in the network. The energy consumption is a critical issue in the design of the Ad-hoc networks.The mobile devices usually have limited storage and low computational capabilities. They heavily depend on other hosts and resources for data access and information processing. A reliable network topology must be assured through efficient and secure routing protocols for Ad-hoc networks.

The Following Are The Advantages of Manets

1. They provide access to information and services regardless of geographic position.
2. These networks can be set up at any place and time.

The mainstay of this project is to design a neighbor coverage based probabilistic rebroadcast (NCPR) protocol for MANET.

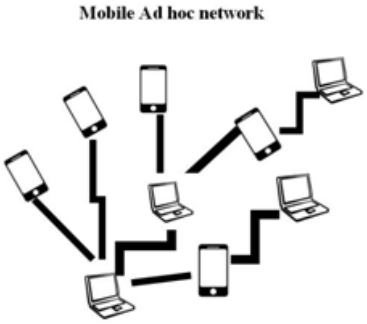


Fig.1.1 Mobile Ad-hoc Network

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing.However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs.Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns.Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

1.3 Application areas

Some of the applications of MANETs are

1. Military or police exercise.
2. Disaster relief operation.
3. Mine site operation.

4. Urgent Business meetings.
5. Robot data acquisition.

It is easy to imagine a number of applications where this type of properties would bring benefits. One interesting research area is inter-vehicle communication. It is one area where the Ad-hoc networks could really change the way we communicate covering personal vehicles as well as professional mobile communication needs.Also, it is area where no conventional (i.e.wired) solution would do because of the high level of mobility. When considering demanding surroundings, say mines for example, then neither would the base station approach work but we must be able to accomplish routing via nodes that are part of the network .i.e. we have to use Ad-hoc network.Such networks can be used to enable next generation of battlefield applications envisioned by the military including situation awareness systems for maneuvering war fighters, and remotely deployed unmanned micro-sensor networks. Ad-hoc networks can provide communication for civilian applications, such as disaster recovery and message exchanges among medical and security personnel involved in rescue missions.

1.4 AD-HOC networks VS mobile Ad-hoc networks

Ad-hoc networks form spontaneously without a need of an infrastructure or centralized controller. This type of peer-to-peer system infers that each node, or user, in the network can act as a data endpoint or intermediate repeater. Thus, all users work together to improve their liability of network communications.

These types of networks are also popularly known to as "mesh networks" because the topology of network communications resembles a mesh. The redundant communication paths provided by Ad-hoc mesh networks drastically improve fault tolerance for the network. Additionally, the ability for data packets to "hop" from one user to another effectively extends the network coverage area and provides a solution to overcome non-line of sight (LOS) issues.Mobile applications present additional challenges for mesh networks as changes to the network topology are swift and widespread. Such scenarios require the use of Mobile Ad-hoc Networking (MANET) technology to ensure communication routes are updated quickly and accurately.MANETs are self-forming, self-maintained, and self-healing, allowing for extreme network flexibility. While MANETs can be completely self contained, they can also be tied to an IP-based global or local network (e.g. Internet or private networks). These are referred to as Hybrid MANETs.As you can see above we have three self-configuring mobile routers connected by wireless links creating MANET. However, as the routers approach the other two IP-based global or local netwrks; they form a network which connects them all through those other networks, forming a hybrid MANET.A Mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form a random topology. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make Ad-hoc networks suitable for emergency situations like natural or man induced disasters, military conflicts, emergency medical situations etc.

1.5 Pro's and Con's

1. The network can be set up at any time and place.
2. Independence from central network administration
3. Self-configuring network, node are also act as routers
4. Less expensive as compared to wired network
5. Scalable-accommodates the addition of more nodes
6. Improved Flexibility
7. Robust due to decentralize administration
8. The nodes can combine and leave at anytime
9. If any nodes tends to fail the entire networks will be affected

II. Literature survey

2.1 A Practical Approach For Provenance Transmission "S. Alam And S. Fahmy"

In this project [11], we presented an energy-efficient provenance transmission and construction approach for large-scale multi-hop wireless sensor networks, based on the idea of probabilistic incorporation of node identities. We adapt the Probabilistic Packet Marking (PPM) approach for IP traceback, and propose three provenance encoding methods with a space constraint on the size of provenance data in each packet. We analyze the suitability of the methods based on the network size and bit budget via mathematical approximations and numerical methods. In contrast to PPM, our proposed approach requires fewer packets to construct network-wide provenance, and significantly reduces the aggregate energy consumption of the network, as demonstrated via both simulations and testbed experiments. We also incorporate a simple but robust scheme into PPF to

handle topological changes. PPM variants do not consider such changes. We demonstrate the effectiveness of PPF in highly dynamic and asymmetric networks using simulation and tested experiments. PPF integration with a provenance-based trust framework reveals no degradation in accuracy of trust scores. We also explore the trade-off between trustworthiness or provenance dissimilarity of data items and transmission overhead. In this regard, we propose a solution to provide decision makers with a tunable parameter to control the extent of provenance dissimilarity and transmission overhead.

2.2 Technique Used

Probabilistic Packet Marking Technique

2.3 Drawback

The existing system failed to discover all neighbor nodes for each nodes, thus results in affecting the packet delivery ratio and increase in time delay with constraint packet losses.

2.3 Network Applications Of Bloom Filters "A. Broder And M. Tzenmacher,"

In this paper [12], A Bloom filter is a simple space-efficient representation of a set or a list that handles membership queries. As we have seen in this survey, there are numerous networking problems where such a data structure is required. Especially when space is an issue, a Bloom filter may be an excellent alternative to keeping an explicit list. The drawback of using a Bloom filter is that it allows false positives. Their effect must be carefully considered for each specific application to determine whether the impact of false positives is acceptable. This leads us back to: The Bloom filter principle: Wherever a list or set is used, and space is at a premium, consider using a Bloom filter if the effect of false positives can be mitigated. There seems to be plenty of room to develop variants or extensions of Bloom filters for specific applications. For example, we have seen that the counting Bloom filter allows for approximate representations of multi-sets or dynamic sets that change over time through both insertions and deletions. Bloom filters are now starting to receive significant attention from the algorithmic community, and while there have been a number of recent results, there may well be further improvements to be found.

2.4 Technique Used

Bloom Filter Technique

2.5 Drawback

The certificate revocation process tends to take a long time in detecting malicious node.

The existing work doesn't work on eliminating the malicious node.

2.6 Graph Constrained Group Testing "M. Cheraghchi, A. Karbasi, S. Mohajer, And V. Saligrama"

These concepts suggest that the graph constrained group testing [13] problem motivated by applications in network tomography, sensor networks and infection propagation. While group testing theory and its numerous applications, such as industrial quality assurance, DNA library screening, software testing, and multi-access communications, have been systematically explored, the graph constrained group testing problem is new to the best of our knowledge. Non-adaptive group testing involves grouping arbitrary subsets of items into different pools. Each pool is then tested and defective items are identified. A fundamental question involves minimizing the number of pools required to identify at most defective items. Motivated by applications in network tomography, sensor networks and infection propagation, a variation of group testing problems on graphs is formulated. Unlike conventional group testing problems, each group here must conform to the constraints imposed by a graph. For instance, items can be associated with vertices and each pool is any set of nodes that must be path connected. In this paper, a test is associated with a random walk. In this context, conventional group testing corresponds to the special case of a complete graph on vertices. For interesting classes of graphs a rather surprising result is obtained, namely, that the number of tests required to identify defective items is substantially similar to what is required in conventional group testing problems, where no such constraints on pooling is imposed.Technique Used Conventional Group Test Technique

2.7 Drawback

GR is very sensitive to the inaccuracy of location information.If the node moves out of the sender's coverage area, the transmission will fail.Due to the error prone wireless channel and the dynamic network topology, reliable data delivery inMANETs, especially in challenged environments with high mobility remains an issue.

2.4 Topological Detection On Wormholes In Manet "D. Dong, M. Li, Y. Liu, X.-Y. Li, And X. Liao, "

In this paper [14], Wormhole attack is a severe threat to wireless Ad-hoc and sensor networks. Most existing countermeasures either require specialized hardware devices or have strong assumptions on the

network, leading to low applicability. In this paper, we fundamentally analyze the wormhole issue by topology methodology and by observing the inevitable topology deviations introduced by wormholes. We generalize the definition of wormholes, classify the wormholes according their impacts on the network, and propose a topological approach. By detecting non separating loops (pairs), our approach can detect and locate various wormholes and relies solely on topological information of the network. To the best of our knowledge, we make the first attempt toward a purely topological approach to detect wormholes distributedly without any rigorous requirements and assumptions. Our approach achieves superior performance and applicability with the least limitations.

2.5 Technique Used
Topological approach

2.6 Drawback
Recognizing that a static allocation of spectrum over time and space is highly suboptimal.

2.7 Understanding Routing Dynamics In A Large-Scale Network"T. Zhu Et Al"

In this paper [2], we present MAP, a methodology for measuring and analyzing the loss performance of a large operating WSN in the wild. Based on the collected data, we present an approach for uncovering the spatial-temporal distributions of the loss events as well as developing a causal graph with which we perform spatial-temporal correlation analysis for revealing the root causes. We summarize implications and lessons learned and give important guidance to future WSN deployments. There are multiple dimensions to explore. First, we would like to examine more number of system events, such as link quality changes, routing dynamics. Second, we would like to implement our methodology as a realtime service, augmented with limited use of passive sniffing or local logging for deep examination of wireless behaviors.

2.8 Technique Used
MALP (Measuring and Analyzing the Loss Performance)
2.9Drawback
It is difficult critical for improving system performance and exploring further development and applications.

III. Existing System

In the existing system, a technique Compressive-Sensing-based Path Reconstruction method, CSPR, this contains the compressive sensing to recover routing paths. It annotates the transmitted and classifies packets traveling along different paths into different groups. This forwarded a packet which encodes levels to perform compressive sensing to recover the path when a certain amount of packets (and the annotations) is collected. The path reconstruction by CSPR requires no interpacket correlations and utilizes only a small number of received packets. CSPR is thus invulnerable to topology dynamics and lossy links and fixed overhead in annotating each packet, which could be optimized WSNs. A set of optimization techniques to gradually shrink the representation space and reduce the sparsity of unrecovered path vectors. The numbers of packets needed for remaining path reconstructions are lowered, and processing is thus accelerated.

3.1 Methodologies used
CSPR (compressive sensing path reconstruction)

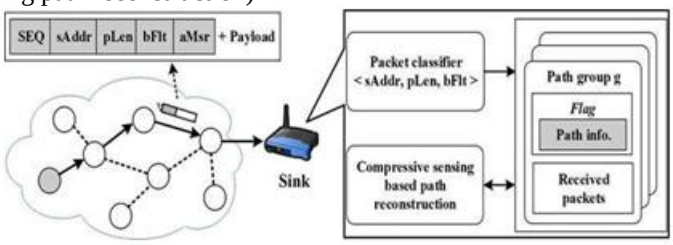
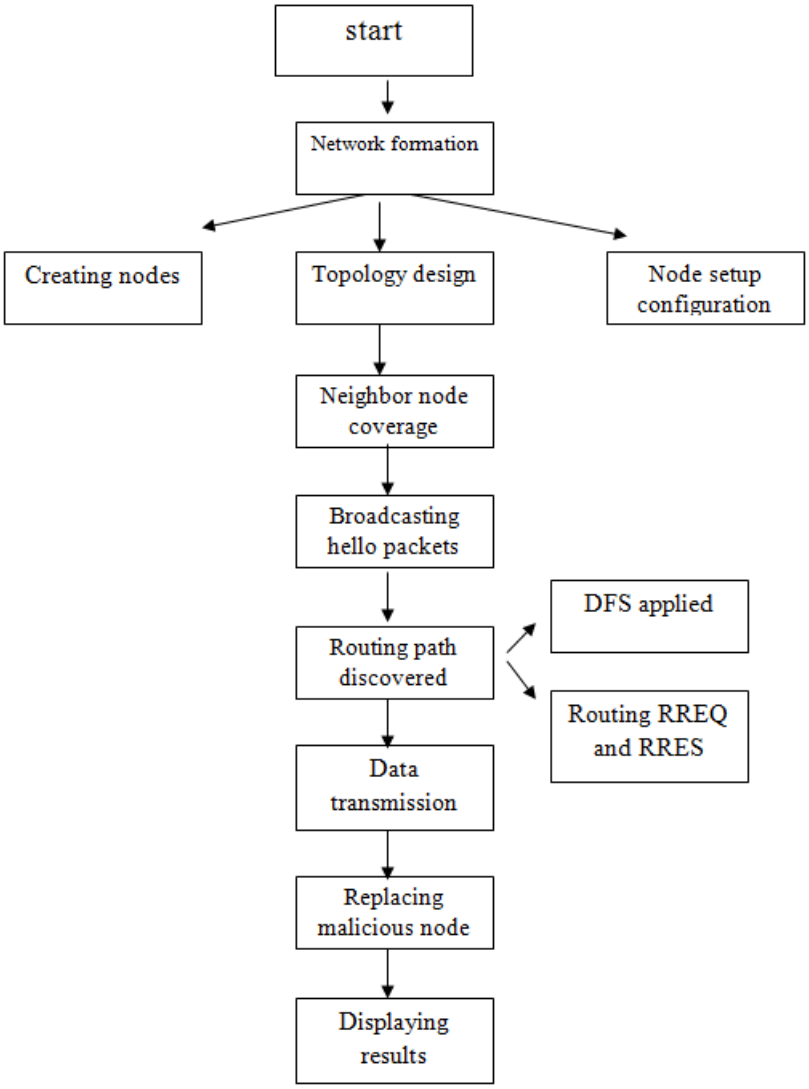


Fig 1.2 Structure of CSPR

3.2 Drawbacks
It has no interpacket correlations and utilizes only a small number of received packets and invulnerable to topology dynamics and lossy links.

IV. Proposed Work

In the system we have implemented a selfish node detection method nd novel replica allocation technique to handle the selfish replica location. The proposed schemes are inspired by the real world observations in economics in terms of credit risk and in human friendship management in terms of choosing one's friends completely at one's own decision. We have applied the concept of credit risk from economics to detect selfish nodes. Each and Every node in a specific network calculates credit risk information on other connected nodes individually to measure the degree of selfishness.The system performance is extensively significant in the detection of attacker and to provide congestion control at MANET. Extensive simulation shows that the proposed strategies outperform the cooperative replica allocation techniques in terms of data accessibility, communication cost, and query delay. The False alarm at selfishness will decrease the data flow of the network. By using our technique we will pass the information as it is not by selfishness. So no significant change will occur except choosing for alternative routes. As a part future, we plan to consider all the replication strategies and network disconnections suited for various consistency levels and with increase in security against various attacks. Our next goal will be to conduct an analytical study of the impact of node mobility on network performance with misbehaving nodes.We plan then to design and evaluate a collaborative security scheme that solves the selfishness problem, analyzing the effects of such mechanism on network throughput and communication delay.



4.1 Algorithm: Proposed FA-REP algorithm based on threshold value in MANETs

Notation: SRN: Source node
DTN: destination node
HV: Threshold Value

1. The SRN broadcasts the packets through all possible paths available in the topology.
2. Finding shortest path through DFS algorithm.
3. The packets have been sending from source to destination.

Calculate the alert value of each node in the network based on the energy, Denial of service, acknowledgment, flooding of messages

1. If the alert value of any node is minimum it will be considered as selfish node.
2. If alert value (alert<THV) then the alert message will be produced.

Snode=Xnode<Tvalue

Where

Snode: Selfish node

Xnode: each node in network

1. Tvalue: Threshold value to be assigned
2. Then the selfish node will be replaced by the active node which is adjacent of source node using replacement algorithm.
3. Allow nodes for trustworthy transmission of packets. End

4.2 Node replacement algorithm

1. Create the network formation in terms of Node configure settings.
2. Sending broadcast message "Hello Packets" to the Network for neighbor coverage.
3. Neighbor Node Phase activated
4. Apply DFS for finding shortest path.
5. Find the malicious node using False Alarm Algorithm
6. Creating the Active node in the nearest Node of source node in network
7. Replacing the selfish node when get alert of malicious node by using NRA.

4.3 Finding the delay time for each routing node.

The delay time is calculated which means each node sends the neighbor discovery phase to neighbors, from the time taken by source node for broadcasting O packets to its neighbor.

ADT=$\sum (T_r-T_s)$/Total data packets received

Where:

ADT: Average delay time

Tr: Time taken to received

Ts: Time taken to sent

V. Simulation Result

Fig.5.1. Performance Assessment chart for FA-REP based on Routing performance

The Performance Assessment of the proposed FA-REP is analyzed by deriving delay time of the network in the above mentioned difference scenarios. The above diagram illustrates the plots depicting throughput values obtained through CSPR with FA-REP. The proposed FA-REP shows considerable increase in the throughput of the entire network. From the result it is clear that the proposed FA-REP approach mitigates and replaces the selfish node that present in the ad hoc network in a rapid manner.

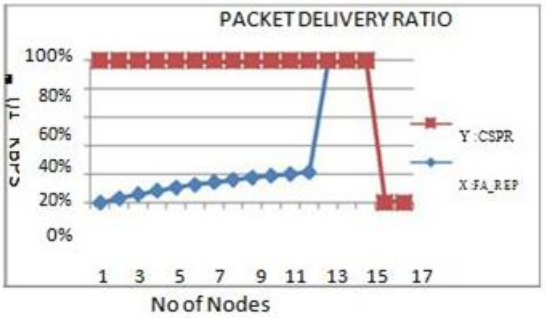


Fig.5.2. Performance Assessment chart for FA-REP based on Packet delivery ratio

The Performance Assessment of the proposed FA-REP is analyzed by deriving throughput of the network in the above mentioned difference scenarios. The above diagram illustrates the plots depicting throughput values obtained through CSPR with FA-REP. The proposed FA-REP shows considerable increase in the throughput of the entire network. From the result it is clear that the proposed FA-REP approach mitigates and replaces the selfish node that present in the ad hoc network in a rapid manner.

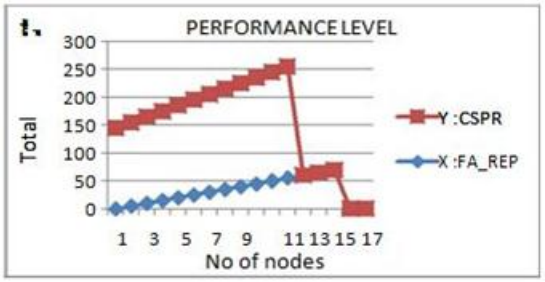


Fig.5.3. Performance Assessment chart for FA-REP based on Performance level

The Performance Assessment of the proposed FA-REP is analyzed by deriving the value of total overhead of the network in the above mentioned difference scenarios. The above diagram illustrates the plots depicting throughput values obtained through CSPR with FA-REP. The proposed FA-REP shows considerable increase in the throughput of the entire network. From the result it is clear that the proposed FA-REP approach mitigates and replaces the selfish node that present in the ad hoc network in a rapid manner.

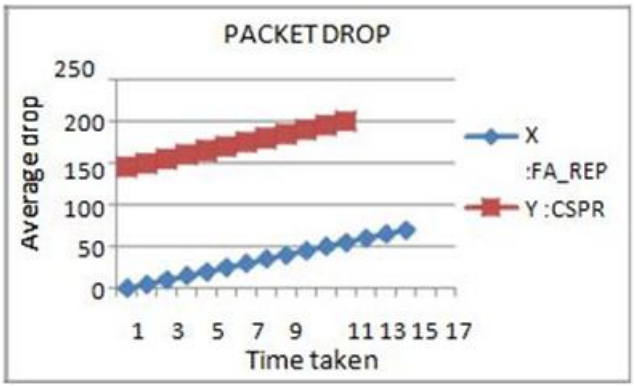


Fig.5.4. Performance Assessment chart for FA-REP based on Packet drop

The Performance Assessment of the proposed FA-REP is analyzed by deriving the value of packet drop of the network in the above mentioned difference scenarios. The above diagram illustrates the plots depicting throughput values obtained through CSPR with FA-REP. The proposed FA-REP shows considerable increase in the throughput of the entire network. From the result it is clear that the proposed FA-REP approach mitigates and replaces the selfish node that present in the ad hoc network in a rapid manner.

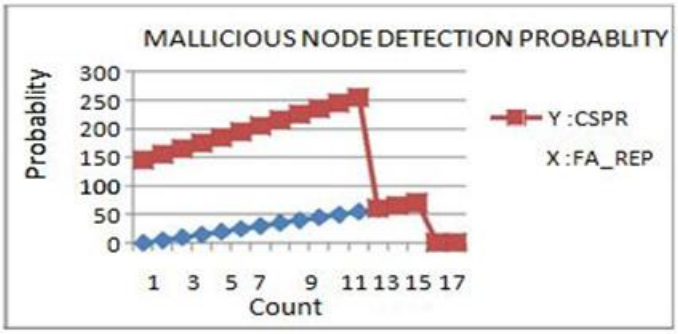


Fig.5.5. Performance Assessment chart for FA-REP based on Malicious node detection probability

The Performance Assessment of the proposed FA-REP is analyzed by means of measuring probability count of the network in the above mentioned difference scenarios. The above diagram illustrates the plots depicting throughput values obtained through CSPR with FA-REP. The proposed FA-REP shows considerable increase in the throughput of the entire network. From the result it is clear that the proposed FA-REP approach mitigates and replaces the selfish node that present in the ad hoc network in a rapid manner.

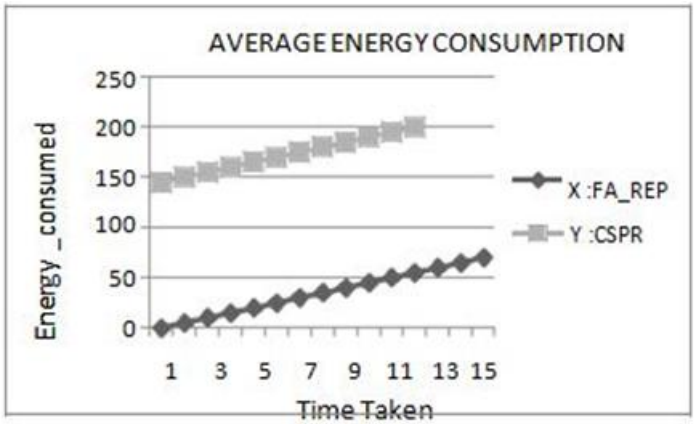


Fig.5.6. Performance Assessment chart for FA-REP based on average energy consumption

The Performance Assessment of the proposed FA-REP is further studied by deriving the value of energy consumed of the network in the above mentioned difference scenarios. The above diagram illustrates the plots depicting throughput values obtained through CSPR with FA-REP. The proposed FA-REP shows considerable increase in the throughput of the entire network. From the result it is clear that the proposed FA-REP approach mitigates and replaces the selfish node that present in the ad hoc network in a rapid manner.

VI. Conclusion

The proposed combined algorithm Node Replacement and False alarm with the decision making based on fuzzy rules has shown more accurate results than the algorithms which have been used alone. By detecting attacks approximately corresponds to the results is obtained to that of the number of lines of code decreased and as well as the opportunity to easily integrate various exterior libraries, thus greatly simplifies the completion of the algorithms and decision-making system. The opportunity provides a unique for efficient detection and inhibition of network security problems, allowing the amalgamation of complex network security applications in large networks.

References

[1]. P. Sattari, A. Markopoulou, C. Fragouli, and M. Gjoka, "A network coding approach to loss tomography," IEEE Trans. Inf. Theory, vol.59, no. 3, pp. 1532–1562, Mar. 2013.
[2]. T. Zhu et al., "Understanding routing dynamics in a large-scale wireless sensor network," in Proc. IEEE MASS, 2013, pp. 574–582.
[3]. Q. Ma, K. Liu, X. Miao, and Y. Liu, "Sherlock is around:Detecting network failures with local evidence fusion," in Proc. IEEE INFOCOM, 2012, pp. 792–800.
[4]. X. Mao, X. ***Li***, Y. He, X. Li, and Y. Liu, "CitySee: Urban CO monitoring with sensors," in Proc. IEEE INFOCOM, 2012, pp. 1611–1619.
[5]. L. Ma, T. He, K. K. Leung, D. Towsley, and A. Swami, "Efficient identification of additive link metrics via network tomography," in Proc. IEEE ICDCS, 2013, pp. 581–590.

[6]. Z. Liu, Z. Li, M. Li, W. Xing, and D. Lu, "Path reconstruction in dynamic wireless sensor networks using compressive sensing," in Proc. ACM MobiHoc, 2014, pp. 297–306..
[7]. Z. Li, M. Li, and Y. Liu, "Towards energy-fairness in asynchronous duty-cycling sensor networks," Trans. Sensor Netw., vol. 10, no. 3, p. 38, 2014.
[8]. L. He et al., "Evaluating service disciplines for on-demand mobile data collection in sensor networks," IEEE Trans. Mobile Comput., vol. 13, no. 4, pp. 797–810, Apr. 2014.
[9]. L. He, J. Pan, and J. Xu, "A progressive approach to reducing data collection latency in wireless sensor networks with mobile elements," IEEE Trans. Mobile Comput., vol. 12, no. 7, pp. 1308–1320, Jul. 2013.
[10]. Y. Liu, K. Liu, and M. Li, "Passive diagnosis for wireless sensor networks," IEEE/ACM Trans. Netw., vol. 18, no. 4, pp. 1132–1144, Aug. 2010
[11]. S. Alam and S. Fahmy. A practical approach for provenance transmission in wireless sensor networks. Ad Hoc Networks, 2013
[12]. Broder and M. Mitzenmacher, "Network applications of bloom filters:A survey," Internet Math., vol. 1, no. 4, pp. 485– 509, 2004.
[13]. M. . Cheraghchi, A. Karbasi, S. Mohajer, and V. Saligrama, "Graph constrained group testing," IEEE Trans. Inf. Theory, vol. 58, no. 1, pp.248–262, Jan. 2012.
[14]. D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor tworks,IEEE/ACM Trans. Netw., vol. 19, no. 6, pp. 1787–1796, Dec. 2011.