ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 5, May 2018

Packet Loss Estimation using Fine Grained Analysis in MANETS

[1] M.Gopinath, [2] R.Maniraj, [3] P.Bharathi
[1] [2] Assistant Professor Department Of Information Technology Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College,Chennai,India
[3] Pg Scholar,Department Of Master Of Computer Application Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College,Chennai,India

Abstract: ***There is also many reasons for packet loss, like interference, queue overflow, and node quality. To discover actually malicious nodes, it's necessary to hold out a fine grained analysis (FGA) theme to work out underlying causes of such loss. While not such analysis, the performance of any security resolution could degrade, owing to the penalization of innocent nodes whereas actual malicious nodes could stay undetected. Therefore, approaches are needed that may properly establish the explanation for packet losses and might react consequently. During this paper, we have a tendency to gift a theme that's ready to properly establish malicious nodes, victimization network parameters to work out whether or not packet losses are owing to queue overflows or node quality in MANETs. The contributions of this paper embody the FGA theme for packet loss and therefore the development of a comprehensive trust model for malicious node identification and isolation. Our projected FGA theme is evaluated in terms of effectiveness and performance metrics beneath totally different network parameters and configurations. The experimental results show that our projected trust model achieves a big reduction in false Positives rate and a rise within the rate of detection of actually malicious and victimization ECC formula to enhance the information speed.***

Index Terms— *FGA scheme, misbehaving node, ECC algorithm, Queue overflow*

I. INTRODUCTION

In Mobile impromptu Network (MANET) is sorts of impromptu networks they will use wireless association to attach to numerous networks a collection of mobile nodes are connected via wireless link in AN infrastructure less network. The network assumptions are elementary for the sort of security mechanism we are able to deploy. Ideally the communication and security properties we would like the network to possess beneath any variety of adversarial setting are: access management, convenience, and finish to finish message integrity, legitimacy, and confidentiality. However, not all of those properties are simply achieved. Some properties even have mutual conflicting goals: providing integrity, legitimacy and confidentiality incur in further computation and information measure from the network, which may manufacture a decrease in network performance, practicality and ultimately, it will have an effect on its convenience.

This network at risk of varied attacks by misbehaving nodes like, (I) a node drops information packets as a result of malicious Behavior; (II) a node provides falsified routing data to order nodes so as to disrupt the network and (III) a node doesn't participate in routing operation so as to save lots of its own energy [1]. To spot and isolate non-cooperative in MANETs, a variety of trust-based security schemes [2]. In MANETs, trust is outlined on what extent a node will fulfill the expectations of another node.

II. RELATED WORK

In existing trust-based security schemes for MANETs, K.Lai,[2]. They projected a watchdog and path-rate mechanism enforced on the DSR protocol to attenuate the impact of malicious nodes on the output of the network. The main defect that every packet drop is taken into account as misdeed by a node no matter the explanation for the packet drop. To handle such shortcomings, varied approached were Proposed, like acknowledgment-based detection schemes as well as TWOACK , AACK. The TWOACK theme was projected to unravel the shortcomings of the watchdog and path-rater theme, like receiver packet collision and restricted transmission power drawback. Within the TWOACK theme, each 3 consecutive nodes within the path from sender to the destination square measure needed to acknowledge each transmitted packet. AN improved version of the TWOACK theme, known as AACK [3]. In MANET's surroundings mistreatment DSA, RSA and error correction code digital signatures. Their technique will validate and attest the acknowledgement packets, however at the expense of additional resources; it conjointly needs Pre-distributed keys for digital signatures.

To estimate the packet loss rate over link, a theme that uses expected transmission count metrics, just like the Excepted Transmission Time (ETT) metric. Such theme with success computes the packet loss rate, however it's unable to spot the particular explanation for packet loss. A fine-grained analysis theme to investigate the packet loss reasons in wireless device networks (WSNs). In such an approach, the parameters used for link identification square measure the received signal strength indicator (RSSI), RSSI is sometimes invisible to a user of a receiving device. LQI (Link Quality Indicator) could be a metric of this quality of the received signal, and also the packet reception rate (PRR) to estimate PRR in dependence of packet size and use this data to schedule transmissions specified delivery magnitude relation is maximized. This Approach is extremely effective for Wireless device Networks that have a comparatively static topology however the identification parameters utilized by this approach can't be simply applied to MANETs that square measure extremely dynamic environments

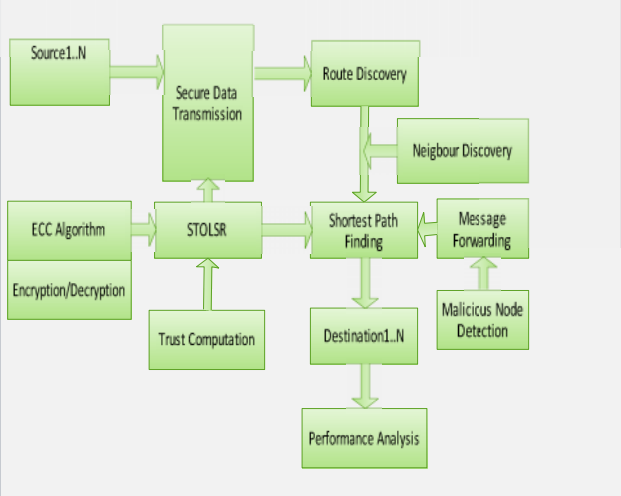
III. PROPOSED SYSTEM

We propose Secure Trust-OLSR (STOLSR) supported cooperation and routing operation and assaulter detection, prevention .we detail the techniques and also the contributions in trust-based security in OLSR.We tend to gift trust-based analysis of the OLSR protocol victimization trust specification language which we tend to show but trust-based reasoning can allow each node to measure the behaviour of the alternative nodes. When the detection of misbehaving nodes, we tend to propose solutions of bar and countermeasures to resolve the things of inconsistency, and counter the malicious nodes. We tend to projected cryptography based mostly security mechanism to security algorithms like ECC Security algorithmic program. ECC is understood for each its tremendous speed and overall effectiveness as several claim that it's ne'er been defeated. Rising coding and decoding aspects of the algorithmic program, that is exist already and creates the manner for a wonderful security.

ADVANTAGES

FGA sight false positives, detection rate, and packet loss rate with increasing rate, node speed, and node degree. Reduction in false positives rate and a rise within the rate of detection of really malicious nodes. Trusty nodes and excellent IDSs' Reduces the IDSs' active time the maximum amount as attainable while not compromising on its effectiveness. Increasing the period of the network and achieved security level considerably. Overall energy consumption is reduced and will increase network performance.

ARCHITECTURE DIAGRAM



IMPLIMENTATION

This is developed to MANET networksdata communication and aggregation process. The radio and IEEE 802.11 MAC layer models were used. The network based data processing or most expensive and data communication level on their performance on the network. Multiple sources create and end sending packets; each data has a steady size of 512 bytes.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 5, May 2018

Trust Computation

To make a security call with the computed trust worth, we'd like to estimate what proportion risk is reasonable for every in progress task. In alternative words, a threshold of trust worth (Threshold) must be outlined for every task. Such threshold trust worth is also varied looking on the safety demand of every in progress task. By comparison the computed trust worth and therefore the threshold trust worth, it's straightforward to examine whether or not the trustee node satisfies the trust demand or node.

Trust computation based attacker detection

T^{d}_{ij}-Trust value

I and j nodes

α-positive value

B-negative value

Trust value=10/10+8

=10/18

=0.5

Formula:

$$T^{d}_{ij} = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}}$$

STOLR

This is developed to propose Secure Trust-OLSR (STOLSR) supported cooperation and routing operation and assaulter detection, prevention .we detail the techniques and also the contributions in trust-based security in OLSR[6]. We have a tendency to gift trust-based analysis of the OLSR protocol victimization trust specification language and that we show however trust-based reasoning will enable every node to gauge the behavior of the opposite nodes

DSR:

The Dynamic source Routing Protocol [5] is one among the on-demand routing protocols, and is predicated on the conception of supply routing. In supply routing, a sender node has within the packet header the whole list of the trail that the packet should jaunt the destination node. That is, each node within the path simply forwards the packet to its next hop laid out in the header while not having to ascertain its routing table as in table-driven routing protocols. Besides, the nodes don't have to be compelled to sporadically broadcast their routing tables to the neighbouring nodes. This protects lots of network information measure. The 2 phases of the DSR operation area unit delineate below:

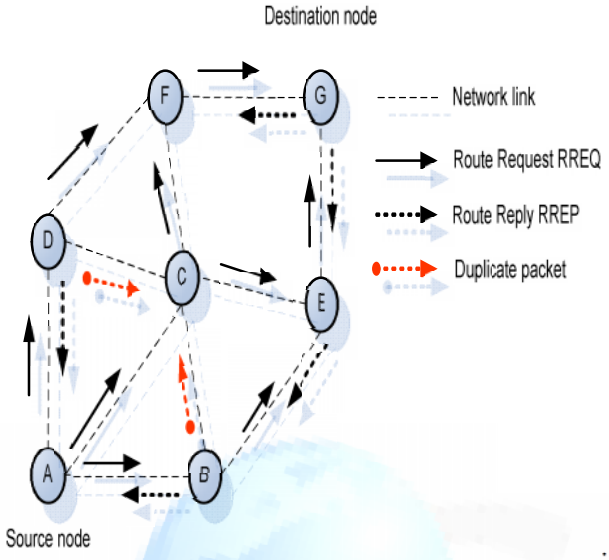
- Route Discovery
- Route maintenance

Route discovery:

In this section, the supply node searches a route by broadcasting route request (RREQ) packets to its neighbors. every of the neighbor nodes that has received the RREQ broadcast then checks the packet verify to work out to see that of the subsequent conditions apply: (a) Was this RREQ received before? (b) is that the TTL (Time To Live) counter bigger than zero? (c) Is it itself the destination of the RREQ? (d) Ought to it broadcast the RREQ to its neighbors? The request ids area unit accustomed determines if a selected route request has been antecedently received by the node. Every node maintains a table of RREQs recently received. Every entry within the table could be a try. If 2 RREQs with constant area unit received by a node, it broadcasts solely the one received 1st and discards the opposite. This mechanism additionally prevents formation of routing loops inside the network. Once the RREQ packet reaches the destination node, the destination node sends a reply packet (RREP) on the reverse path back to the sender. This RREP contains the recorded route to its destination.When node A needs to speak with node G, it initiates a route discovery mechanism and broadcasts asking packet (RREQ) to its neighboring nodes B, C and D as shown within the figure1.1. However, node C conjointly receives an equivalent broadcast packet from nodes B and D. It then drops each of them and broadcasts the antecedently received RREQ packet to its neighbors. The opposite nodes follow an equivalent procedure. once the packet reaches node G, it inserts its own address and reverses the route among there cord and uncast it back on the reversed path to the destination that's that the creator of the RREQ. Don't have any text to check? Don't have any text to check?

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 5, May 2018

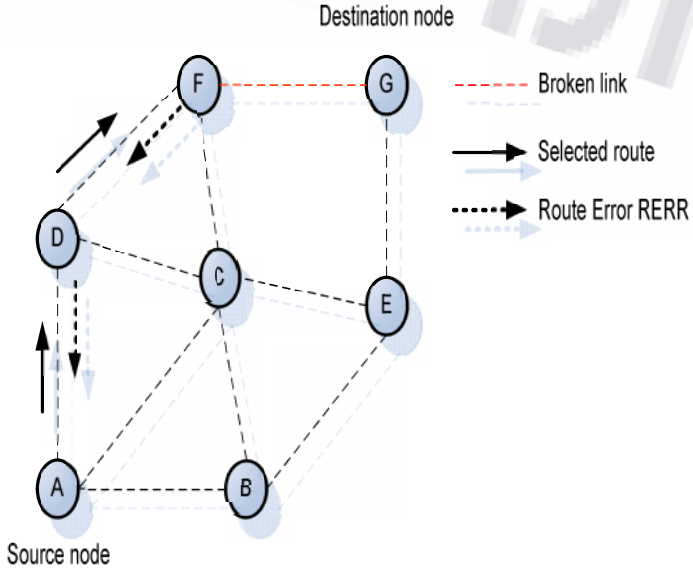
Click "Select Samples". The destination node uncast the simplest route (the one received first) and caches the opposite routes for future use. A route cache is maintained at each node so, whenever a node receives a route request and finds a route for the destination node in its own cache; it sends a RREP packet itself rather than broadcasting it additional



1.1 Route Discovery in DSR

Route maintenance

The route maintenance part is dispensed whenever there's a broken link between 2 nodes. A broken link is detected by a node by either passively observance in promiscuous mode or actively observance the link. As shown in Figure1.2. A pair of.3, once a link break (F-G) happens, a route error packet (RERR) is distributed by the intermediate node back to the originating node. The supply node re-initiates the route discovery procedure to search out a brand new route to the destination. It conjointly removes any route entries it should have in its cache to its destination node.



1.2 Route Maintenance in DSR

DSR advantages from supply routing since the intermediate nodes don't got to maintain up-to-date routing data so as to route the packets that they receive. There's conjointly no want for any periodic routing advertisement messages. However, as size of the network will increase, the routing overhead will increase since every packet should carry the complete route to the

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 5, May 2018

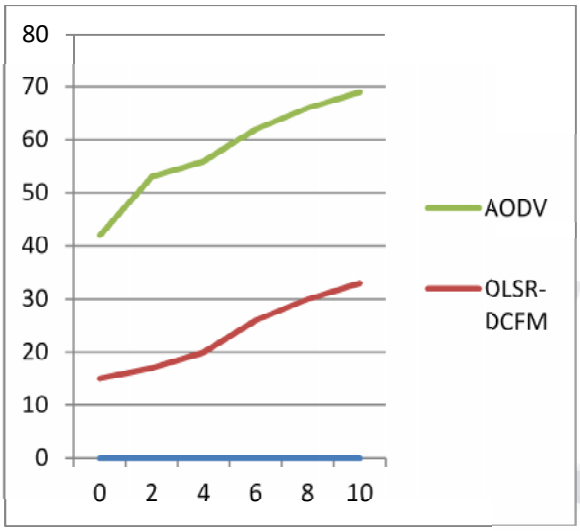
destination alongside it. the utilization of route caches could be a smart mechanism to scale back the propagation delay however overuse of the cache could end in poor performance [4]. Another issue of DSR is that whenever there's a link break, the RERR packet propagates to the first supply that successively initiates a replacement route discovery method. The link isn't repaired regionally. many optimizations to DSR are projected, like non- propagating route requests (when causing RREQ, nodes set the hop limit to at least one preventing them from re-broadcasting), gratuitous route replies (when a node overhears a packet with its own address listed within the header, it sends a RREP to the originating node bypassing the preceding hops), etc. an in depth clarification of DSR optimizations is found in [5].

Ad-hoc On-demand Distance Vector (AODV) routing protocol

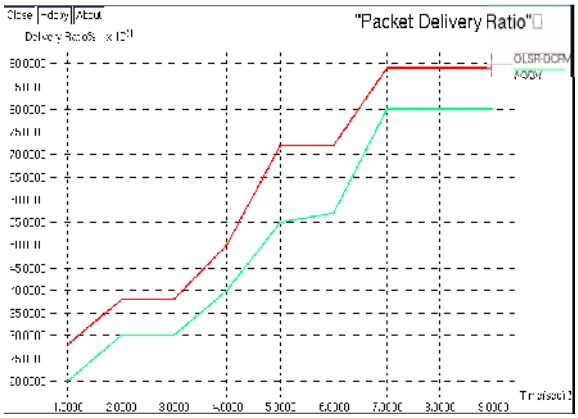
To seek out routes, the AODV routing protocol [7] uses a reactive approach and to spot the foremost recent path it uses a proactive approach. That is, it uses the route discovery method the same as DSR to seek out routes and to figure recent routes it uses destination sequence numbers.

Performance Analysis Result

Developed to enhance Wireless network performance, scale back Average finish –to-end delay.



1.3 Average End-to-End Delay



1.4. Packet Delivery Ratio

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 5, May 2018

ECC Algorithm:

Attack prevention model

Cryptographic technique used here is elliptic curve cryptography. ECC was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography. The equation of an elliptic curve is given as,

$Y^{2=}x^3+ax+b$

Few terms that will be used are,

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (This should be a prime number)

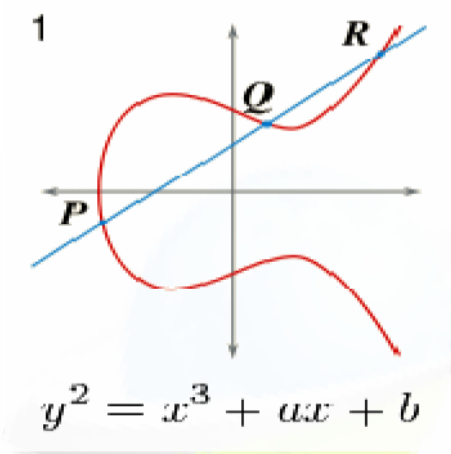


Fig 1.5 simple elliptic curve

GENERATION OF KEY

Generation of key is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number**'d'** within the range of **'n'**.

Using the following equation we can generate the public key

- **Q=d*p**
- **'d '**is the random number that we have selected within the range of (**1 to n-1**). **'P'** is the point on the curve.
- **'Q' is the public key** and**'d' is the private key.**

ENCRYPTION

Let 'm' be the message that we are sending. We have to represent this message on the curve. These have in-depth implementation details.

- Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from; [1 – (n-1)].
- Two cipher texts will be generated let it be **C1** and **C2**.
- **C1 = k*P**
- C2 = M + k*Q
- C1 and C2 will be send.

DECRYPTION

We have to get back the message 'm' that was send to us,

M = C2 – d * C1

M is the original message that we have send. **PROOF**

How does we get back the message,

M = C2 – d * C1

'M' can be represented as 'C2 – d * C1'

C2 – d * C1 = (M + k * Q) – d * (k * P)

Since ,(C2 = M + k * Q and C1 = k * P)

=M + k * d * P – d * k * P (canceling out k * d * P)

= M (Original Message)

This specified mechanism how a packet of data is sent from source to destination. Source nodes encrypt the message using ECC algorithm. The encrypt message is transferred in data packets along the randomly selected path. Other nodes cannot see what is being transferred in the packets. Once data packets reached the destination, data are decrypted in the destination node using the cipher key. Message sent from source is received in destination without loss or damage to data.

IV. CONCLUSION & FUTURE ENHANCMENT:

STOLSR performs higher knowledge Transmission method, because it contains improved aspects of algorithmic rule that is already existed with increased attack detection system. However, the projected attack detection system concentrates solely on the outsider attacks, Future sweetening will be done on considering the corporate executive attacks too which might be done by augmenting the correct authentication schemes that corporate executive nodes cannot scan the particular info.

REFERANCE

[1]. A. A. Cardenas, N. Benammar, G. Papageorgiou,and J.S. Baras, "Cross-layered security analysis of wireless ad-hoc networks," Technical report, DTIC Document, 2004.

[2]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigatingrouting misbehavior in mobile ad hoc networks," inproceedings of the 6th annual ACM Intl. conference onMobile computing and networking, 2000.

[3].K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detectionof routing misbehavior in MANETs," IEEE Transactionson Mobile Computing, 6(5):536-550, 2007

[4].A. Liu, X. Jin, G. Cui, Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network," Information Sciences, vol. 230, pp.197-226, 2013.

[5].Z. Zheng, A. Liu, L. Cai, et al. "Energy and Memory Efficient Clone Detection in Wireless Sensor Networks," IEEE Transactions on Mobile Computing.vol. 15, no. 5, pp. 1130-1143, 2016.

[6]. N. Schweitzer, A. Stulman, A. Shabtai, and R. D. Margalit,"Mitigating denial of service attacks 10 in olsrprotocol using fictitious nodes," IEEE Transactions on
Mobile Computing, 15(1):163-172, 2016.

[7].T. Shu, M. Krunz, S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941-954, 2010.

[8]. P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015.

[9]. C. Zhu, H. Nicanfar, V. C. M. Leung, et al. "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 118-131, 2015.

[10]. Y. Hu, M. Dong, K. Ota, et al. "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency," IEEE System Journal, Doi: 10.1109/JSYST.2014.2308391, 2014.

[11]. T. Clausen, C. Dearlove, P. Jacquet, "The optimized linkstate routing protocol version 2," draft-ietf-manet-olsrv2-00, 2006.