International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 8 (2016) pp 5863-5868

ENES: Exploratory Node Eminence State for Secure Routing in Mobile Ad hoc Networks

G. Soma Sekhar
Research Scholar,
Department of CSE, Acharya Nagarjuna University, India

Dr. E. Sreenivas Reddy
Professor,
College of Engineering, Acharya Nagarjuna University, India

Abstract
The divergent properties such as "adaptive topology", "wireless connectivity" and "dynamic node join and leave" of mobile ad hoc networks open doors for several security vulnerabilities. The ongoing research given considerable attention on Trusted and reputation based node selection in order to establish secure and reliable route. However, these mechanisms compromised to the specific attacks like Eminence Tainting and Colluded Eminence Boosting, which easily degrade the effectiveness of trust and reputation based route discovery models. Hence it is obvious that proposal of novel and robust trust and reputation based secure route discovery is still a considerable research objective.This article proposed a multi-objective model that aimed to identify the eminence state of a node involved in route. The factors "global eminence", "local eminence", "eminence update frequency" and "eminence update diversity" are proposed as multi-objectives to estimate the eminence of the node. Along the side the proposed model also alert to defend the attacks such as "bad mouthing", "colluding", "ballot stuffing". This multi-objective model proposed in this article is labeled as Exploratory Node Eminence State (ENES) for Secure Routing in Mobile Ad hoc Networks that signifies the impact of node eminence to achieve optimal routing. The experimental study of the proposed model evincing the significance of the proposal to achieve optimal routing in mobile ad hoc network with malicious and compromised nodes. The discovered route optimality is evinced by the maximal packet delivery ratio and throughput and minimal end-to-end delay observed. The other critical factor process complexity is found to be linear for proposed model called ENES.

Keywords: **Secure Ad hoc routing, Reputation based node selection, Eminence Tainting, Colluded Eminence Boosting.**

INTRODUCTION

The properties such as "dynamic topology", "loosely coupled network connectivity", "limited infrastructure based network architecture" "network enabled node mobility", "dynamic node join or exit" are evincing the rapid growth in the usage of mobile ad hoc networks by divergent fields with the need of computer and communication networks (P. Michiardi, 2002). Contrast to the above, these ad hoc network properties evincing the several security breaches such as, scope to the malicious and compromised nodes involvement in the routes discovered for data transmission (Conti, 2014). Indeed, these malicious nodes often disrupt the fundamental network operations and also leads to security issues with high severity such as route dropping, intentional denial of packet forwarding, compromised authentication and poor data confidentiality.

The usual way of overcoming these security breaches is that avoiding the routes those contains compromised and malicious nodes. In order to notice such nodes, the current prominent approach is estimating the eminence of the nodes involved in discovered routes.

RELATED WORK

The key exchange and management, hefty cryptographic strategies are the prime factors adopted by traditional research contributions in order to define secure network routing approaches(T. Ghosh, 2004) (T. Ghosh., 2005) (P. Narula, 2008) (Mehra, 2009). These strategies are not fit well to achieve secure routing in mobile ad hoc networks, since the lack of centralized monitoring system, its ad hoc structure that formed with limited resources and minimal computational abilities. Hence it is obvious to invite research contributions in robust secure routing strategies those fit to mobile ad hoc networks and delivers scalability. In order to this a set of benchmarking secure routing strategies for mobile ad hoc networks were evinced in literature of last decade. This section explores these existing set of models to identify the limits and research scope.

Trust based DSR(Pirzada, 2007)is a protocol for discovering routes in the presence of malicious nodes. The nodes monitors the activities of their neighbor nodes and defines their trust levels. The trust levels of the nodes further uses to select optimal route. This model is highly influenced by the attacks such as trust polluting, colluded trust boosting and ballot stuffing.

DMTR (C. Huang, 2007) is the barrel theory based trusted routing protocol.DMTR uses the process of Trust Network Connect (TNC) in order to improve the route security. The concept TNC enables nodes to exchange trust tables, which

deserves substantial bandwidth and leads to cumbersome process overhead.

Estimating the reputation of a node by its behavior is the prime objective of the trust based secure routing model(G. Bella, 2009). This model further rationalizes the observed reputation of a node by the reputation given by other nodes to the target node. This model is also the victim of the attacks such as reputation polluting, colluded reputation boosting and ballot stuffing.

AOTDV(X. Li, 2010)is a trust based secure routing protocol for ad hoc networks.The factors that used in AOTDV to estimate the trustworthiness of a node are forwarding ratio. The multi criteria decision analysis (weighted sum approach) (Sarwar, 2001) was used to find the forwarding ratio, which is used as node trust and continued product (product of node trusts of all nodes involved in that route) of node trusts is considered as route trust. Here, the node is considered as malicious based on its forwarding behavior. In order to identify the forwarding ratio as node trust, the control packet forwarding is weighted minimal that compared to data packet forwarding. The model evinced process overhead and failed to notice the nodes become attacking prone after having considerable forwarding ratio.

The trust scheme (Y. Khamayseh, 2012) is another benchmark model that estimates the credibility of the routes discovered by route request. In order to this, the trust scheme observes the overall behavior of the route and avoids if that route found to be attack prone. This trust scheme is not able to find the credibility of the node. Hence the routes suggest as credible are less optimal, if any of the node turn to be attack prone.

The ratio of response packets against request packets is considered to identify the attack prone nodes, in particular to identify the nodes intended to black-hole attack is another contribution (I. Woungang, 2012) found in recent literature. This ratio of request and response packets is assessed for each node and if that ratio is beyond the threshold value, then that node will be discarded from route discovery process.Due to the process of request and response ratio calculation for each node and caching these ratios for each node, the proposed model is effected by substantial process overhead. This model also failed to identify the nodes committed to black-hole attacks only to neighbor nodes (responds only to the route requests to their neighbor nodes).

An active approach to discover attack prone nodes while routing is on (Arya, 2012) is one, which is detecting node credibility that involved in routing, if node found to be attack prone then switches to alternative route. This approach can be adopted for any of traditional routing strategies like DSR(Abolhasan, 2004) and AODV(Perkins, 2003). The key factors used in this approach are cryptographic approach and flow maintenance at network layer. Due to the hefty cryptographic approach this model is process overhead prone and not robust for networks with hefty attack prone nodes.

EAACK (Shakshuki, 2013)is secure routingSystem for MANETs. The nodes those compromised with malicious activity will be identified in three phases by EAACK. These phases are acknowledging (ACK), Acknowledging Security(S-ACK) and substantiating the mischief (Misbehavior Report Authentication (MRA)). The strategic three phase approach adapted in EAACK is effective to prevent node's those compromised to Black-Hole attack while forming optimal route. The overall process is in three phases and for each phase process overhead observed and not scalable for networks with hefty count of malicious nodes.

Inspired from these novel works, we have implemented one reputation-based scheme for selfish node detection and avoidance of those selfish nodes in case of further data transmission.

EXPLORATORY NODE EMINENCE STATE

The proposal estimates the eminence scope (see sec 3.2) of a node by different metrics proposed (see sec 3.1). The metrics those proposed to use in eminence scope verification are aimed to protect from the different attacking strategies (see sec 3.5) observed in trust based secure routing models. The conditional acceptance of the eminence score update by the nodes involved in routing is another common limit of these trust based secure routing models. This limit also overcome by the ENES through the adapted technique called camouflage publishing strategy (see sec 3.4)

Metrics to estimate the eminence

- Eminence Score (es): The overall eminence score of the node during its lifespan in the network. This can be a negative or positive integer that frequently updated by the source node of the route, which is done upon completion of the routing process. This update is done by adding either 1, 0 or -1 (detailed exploration given in sec 3.3).
- Eminence Update Occurrence Count (uc): This Indicates the count of eminence score update events occurred for a node. This metric reflects the number of times that eminence score got updated.
- Eminence update frequency (uf): The ratio of eminence update occurrences against count of route responses sent regardless that node involved in routing or not.
- Eminence update diversity (ud): The ratio of unique source nodes involved in eminence score update of a node against total number of eminence score update occurrences.

All of the above metrics are optimal at higher values and these metric values are normalized to the value > 0 and ≤ 1

Assessing the route eminence scope

Let a source node isu performs conditional broadcasting [citation required] to identify the possible routes for transmitting data to the target node. Every node involved in Route response includes their "eminence score (es)", "route response count (rrc)", "no of times involved in routing (rc)", "list of unique sources updated its eminence score (unl)".The selection process selects the optimal route that farmed by the nodes with maximum eminence score among all possible routes. The source node assesses conduct sensitivity of the neighbor as follows:

The metrics explored in section 3.1 will be measured for each node that sends route response to source node will be measured as follows

Initially the values received from each node through route response will be verified for their credibility, which is as follows:

The hash of the respective values sent by node n_i will be found initially, then this resultant hash is used as signature and cross checks this signature with the one that already published earlier. If signature is not valid then respective route will be discarded.

The eminence score $ns(n_i)$ received from node n_i is the aggregation of the number of times incremented by 1 ($ns_+(n_i)$, number of time incremented by 0 ($ns_0(n_i)$, number of times incremented by -1 ($ns_-(n_i)$.

Further the ratio of $ns_+(n_i), ns_0(n_i), ns_-(n_i)$ will be measured as

$$\rho_+(n_i) = \frac{ns_+(n_i)}{ns(n_i)}$$

$$\rho_0(n_i) = \frac{ns_0(n_i)}{ns(n_i)}$$

$$\rho_-(n_i) = \frac{ns_-(n_i)}{ns(n_i)}$$

Overall ratio of eminent score $\rho(n_i)$ will be measured as

$$\rho(n_i) = \rho_+(n_i) + \rho_0(n_i) + \rho_-(n_i)$$

Further the ratio of eminence score $ns_+^\tau(n_i), ns_0^\tau(n_i), ns_-^\tau(n_i)$ of recent temporal threshold τ given as.

$$\rho_+^\tau(n_i) = \frac{ns_+^\tau(n_i)}{ns^\tau(n_i)}$$

$$\rho_0^\tau(n_i) = \frac{ns_0^\tau(n_i)}{ns^\tau(n_i)}$$

$$\rho_-^\tau(n_i) = \frac{ns_-^\tau(n_i)}{ns^\tau(n_i)}$$

Further the Current Eminence State of the node n_i is calculated as

$$ces(n_i) = \begin{cases} if \quad \rho_+^\tau(n_i) + \rho_0^\tau(n_i) + \rho_-^\tau(n_i) \le \rho(n_i) \\ \dfrac{\rho_+^\tau(n_i) + \rho_0^\tau(n_i) + \rho_-^\tau(n_i)}{\rho(n_i)} \\ else\ if \quad \rho_+^\tau(n_i) + \rho_0^\tau(n_i) + \rho_-^\tau(n_i) > \rho(n_i) \\ 1 - 1 \Big/ \dfrac{\rho_+^\tau(n_i) + \rho_0^\tau(n_i) + \rho_-^\tau(n_i)}{\rho(n_i)} \end{cases} \quad \text{(Eq1)}$$

// $if \quad \rho_+^\tau(n_i) + \rho_0^\tau(n_i) + \rho_-^\tau(n_i) > \rho(n_i)$, the $ces(n_i)$ is normalized to the value between 0 and 1

The eminence update occurrence count (uc) will be measured as

$$uc(n_i) = 1 - \frac{1}{rc(n_i)} \quad \text{(Eq2)}$$

// $rc(n_i)$ is number of times node n_i involved in routing

The eminence update frequency (uf) of the node n_i will be measured as

$$uf(n_i) = \frac{rc(n_i)}{rrc(n_i)} \quad \text{(Eq3)}$$

// $rrc(n_i)$ indicates the number of times route response sent by node n_i such that $rc(n_i) \le rrc(n_i)$

Further the eminence update diversity (ud) is measured as

$$ud(n_i) = \frac{|unl(n_i)|}{rc(n_i)} \quad \text{(eq4)}$$

// $unl(n_i)$ is unique node list and $|unl(n_i)|$ is unique nodes count those involved in updating eminence score of the node n_i

Further the overall eminence scope of the node n_i is measured as follows

$$ES(n_i) = 1 - ces(n_i) \otimes uc(n_i) \otimes uf(n_i) \otimes ud(n_i) \quad \text{(Eq5)}$$

//Since the values observed for all the metrics normalized to the value > 0 and ≤ 1. The absolute product delivers the value between 0 and 1, which is lesser than any of the metric value, hence the absolute product result subtracted from the 1 to obtain maximum value.

For each route $\{r \exists r \in R\}$ // R is set routes found in route discovery

$$ES(r) = \frac{\sum_{i=1}^{|r|} ES(n_i) \exists n_i \in \{r\}}{|r|} \quad \text{(Eq6)}$$

Further, the eminence scope absolute deviation(Carmines, 1979) for each route r will be measured as follows

$$ead(r) = \frac{\sum_{i=1}^{|r|} \sqrt{ES(r) - ES(n_i)^{\,2}}}{|r|} \quad \text{(Eq7)}$$

//$|r|$ is total number of nodes in route r, $\{r\}$ is set of nodes involved in route r

Further the optimal route selection from the set of routes R discovered will be done as follows:

- Initially the routes in R will sorted in descending order of their respective $ES(r)$ value.
- Then the set of routes those are having $ES(r)$ greater than the given threshold value ϖ .
- Though the eminence scope of route is high, but the deviation of the eminence scope at node level must be low, hence the selected set of routes again sorted in ascending order of their respective $ead(r)$
- Further the top most route in the ordered route list is said to be the most trusted secure route among the discovered routes.

1.1 Assessing the current eminence score

- Aptitude Deflection: The downgraded ability of transmission load is (not found, found due shared resource, or found due to malicious activity).

$$iad = \begin{cases} 1 & if\left(\frac{l_{oc}}{l_{ac}} > \tau_a\right) \\ 0 & \left(if\left(\frac{l_{oc}}{l_{ac}} < \tau_a\right)\& \ (resource\ sharing\ is\ true)\right) \\ -1 & \left(if\left(\frac{l_{oc}}{l_{ac}} < \tau_a\right)\& \ (resource\ sharing\ is\ false)\right) \end{cases} \quad \text{(Eq8)}$$

- Consistency Deflection: The poor ingress, egress ratio (not Found, found due shared resource, or found due to malicious activity).

$$icd = \begin{cases} 1 & if\left(\frac{eg_t}{ig_t} > \tau_c\right) \\ 0 & \left(if\left(\frac{eg_t}{ig_t} < \tau_c\right)\& \ (resource\ sharing\ is\ true)\right) \\ -1 & \left(if\left(\frac{eg_t}{ig_t} < \tau_c\right)\& \ (resource\ sharing\ is\ false)\right) \end{cases} \quad \text{(Eq9)}$$

- Rectitude Deflection: The downgraded performance with no external impacts (not Found, found due shared resource, found due to malicious activity)

$$ird = \begin{cases} 1 & if\left(\frac{oh_o}{oh_e} < \tau_r\right) \\ 0 & \left(if\left(\frac{oh_o}{oh_e} > \tau_r\right)\& \ (resource\ sharing\ is\ true)\right) \\ -1 & \left(if\left(\frac{oh_o}{oh_e} > \tau_r\right)\& \ (resource\ sharing\ is\ false)\right) \end{cases} \quad \text{(Eq10)}$$

If no deflection found in aptitude then the inverse of aptitude deflection (iad) will be scored as 1, if deflection found due to shared resources then the inverse of aptitude deflection will be scored 0, if deflection found and no resources were found to be shared then inverse of aptitude deflection will be scored as -1 (See Eq8) Similarly the other two metrics also scored (see Eq9, Eq10).

Then the eminence score of the node will be estimated as follows:

$$es = \begin{cases} \frac{iad + icd + ird}{\sqrt{iad + icd + ird}^{\,2}} & if \quad iad + icd + ird \neq 0 \\ 0 & if \quad iad + icd + ird \equiv 0 \end{cases} \quad \text{(Eq11)}$$

Eminence Score Update

Once the routing process completed on selected route rt_i, the source node sn updates eminence score of the eachnode n_i involved in routing process. The source node sn furnishes the revised eminence score of each n_i by $es(n_i) + es_{rt_i}(n_i)$ (Here $es(n_i)$ is actual eminence score of the n_i, $es_{rt_i}(n_i)$ is eminence score of n_i observed for route rt_i). If the role of the node n_i found to be fair and optimal in route rt_i then the current eminence score $ec(n_i)$ will be incremented by 1, since eminence score of the node n_i in route rt_i found to be 1 (since $es_{rt_i}(n_i) = 1$) (see Eq11), if cooperation of the node n_i found to be not optimal and node n_i is shared it's resources for other routes or activities then no change applied $es(n_i)$, since $es_{rt_i}(n_i) = 0$ (see Eq11), or if cooperation of node n_i is intended to be malicious (not optimal, and not on shred resources) then the eminence score $es(n_i)$ will be decremented by 1, since $es_{rt_i}(n_i)$ is observed to be -1. The eminence score update is done as follows:

The source node sn prepares eminence score update message esu and sends to cooperative node n_i through the current route rt_i, In regard to this, the 'sn' relies on camouflage publishing approach (Unless accept and publish, message cannot be viewed). The eminence score update esu is formed by sn is as follows:

$$rrc(n_i) = rrc(n_i) + 1$$
$$rc = rc(n_i) + 1$$
$$es(n_i) = es_{rt}(n_i) + es(n_i) \quad \text{(Eq12)}$$
$$unl(n_i) = unl(n_i) \bigcup sn$$
$$es'(n_i) = es(n_i)^{\wedge} s$$
$$ees(n_i) = e_{cp}(\{es'(n_i), rrc(n_i), rc(n_i), unl(n_i)\}) \quad \text{(Eq13)}$$
$$sig = h(id(n_i), es(n_i), rrc(n_i), rc(n_i), unl(n_i)) \quad \text{(Eq14)}$$
$$esu(n_i) = \{ees(n_i), sig(n_i)\} \quad \text{(Eq15)}$$

'$ees(n_i)$' is the encrypted format of the new eminence score $es(n_i)$ that XOR with a salt s, $rrc(n_i)$, $rc(n_i)$ and $unl(n_i)$, which encrypted by the private key and eligible decrypt by the public key of the source node. Any of the intermediate node can decrypt and can see the values other than new eminence score, but can't be decrypted again. Further the new signature of the node n_i will be created, which is the hash value of the node id $id(n_i)$, new eminence score $es(n_i)$, $rrc(n_i)$, $rc(n_i)$ and $unl(n_i)$ that are concatenated by a delimiter such as ";". The message esu contains $ees(n_i)$ and $sig(n_i)$.

In order to avoid the conditional acceptance of the new eminence score by the node n_i, the '$es(n_i)$' is XOR with random value. Upon accepting the $esu(n_i)$ by node n_i .sends a acknowledgment to source node sn , upon receiving the acknowledgement, sn reveals the random value s used in XOR operation. Further node n_i decrypts $ees(n_i)$ and then

performs XOR operation on $es'(n_i)$ and s that results actual $es(n_i)$. Afterwards node n_i updates its $es(n_i), rrc(n_i), rc(n_i)$ and $unl(n_i)$.

Upon completion of the updating the eminence score of the node n_i, source node publishes $sig(n_i)$ to all other nodes through message broadcasting strategy.

Prevention of possible attacks in trust based secure routing by ENES

- Eminence Tainting Attack: In this attack, often compromised source nodes, intentionally pollutes the eminence score of the other nodes.
- Colluded Eminence Boosting: This attack is aimed to boost the eminence score of two individual nodes due to the colluding between those two nodes.

These attacks are having least significance in the proposed ENES, since this model is assessing the eminence scope of node by considering the "divergence of the source nodes involved in eminence score update" and "rather the aggregation, average eminence score given by an individual source node" (see sec 3.2). Hence these attack sequences are having null impact on resultant eminence scope.

EXPERIMENTAL STUDY AND RESULTS ANALYSIS

The experimental Setup

The simulation study was conducted to interrogate the performance of the ENES. In order to estimate the significance of the ENES, the traditional metrics such as packet delivery ratio, average delay and transmission overhead were observed and compared with similar benchmarking model called trust scheme (Y. Khamayseh, 2012).These metrics were assessed against the network with nodes compromised for colluding eminence boosting attack and eminence tainting attack, which are specific to trust based securing routing models. The proposed ENES and benchmark trust scheme (Y. Khamayseh, 2012) were applied on traditional route discovery strategy called AODV (Perkins, 2003). The simulation was done by NS2 (Issariyakul, 2011)and the simulation parameters used were explored in table 1.

Table 1: Parameters used in Simulation

Range of Nodes	70 to 210
Node mobility range	Between 1m and 2.0m/sec
MAC	MAC 802.11 DCF
Network range	1000 X 1800 m2
Direct transmission range of the node	27 meter
Transmission Load range	In the range of 0.5 to 1.5 mbps
Bandwidth	2 Mbps
Transmission Type	CBR
Execution time	360 Sec

Performance Analysis

The metric values those collected from the network simulation with divergent ratio of nodes compromised to "Eminence Tainting Attack" and "colluded eminence boosting attack" evinced that ENES is significant with phenomenal performance that compared to trust scheme proposed in (Y. Khamayseh, 2012). The end-to end delay observed for ENES is potentially minimal (see fig 1), which is due to the process of trusted nodes selection to form the route. The packet delivery ratio is also observed to be noteworthy (see fig 2) that compared to trust scheme. The other important metric "process overhead" is also found to be fair enough for ENES (see fig 3).

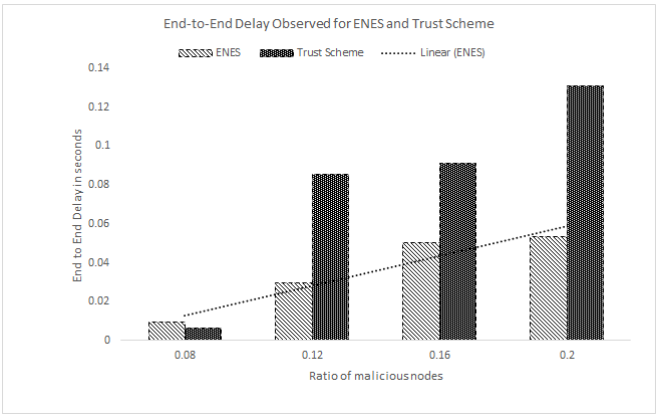

Figure 1: End-to-End Delay observed ENES and Trust-Scheme at divergent pause times

The Trust Scheme delivered downgraded performance under the influence of the eminence tainting and colluding eminence boosting (see fig 1). If malicious nodes ratio is less (0.08) the trust scheme fair enough to restrict the end-to-end delay but failed to maintain the same when ratio of attacking nodes are increased. Whereas the ENES delivers the linearity to restrict end-to-end delay under the sparse to dense ratio of malicious nodes,

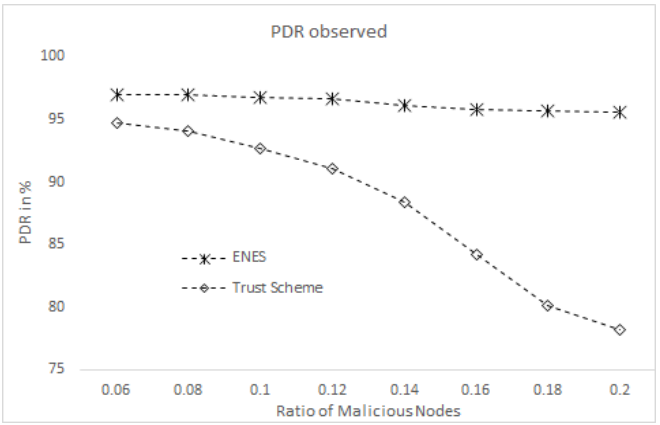

Figure 2: PDR observed for ENES and Trust-scheme

The Fig 2 evincing the inability of the trust scheme to maintain the optimal packet delivery ratio under divergent ratio of attacking nodes. In contrast the ENES is successfully

overcome the influence of malicious nodes and delivers the scalability and robustness in packet delivery ratio (see fig 2).

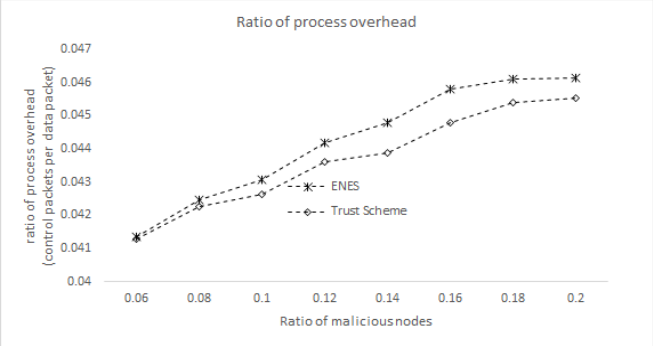

Figure 3: Process Overhead observed for ENES and Trust-Scheme

The ratio of control packets used per each data packet is considered as process overhead. The fig 3 evincing that the process overhead observed for ENES is marginally high that compared to process overhead observed for trust scheme. This is due to the eminence score sharing and camouflage publishing strategy followed in eminence update process. This marginal overhead is trivial in the context of discovering scalable route with robust packet delivery ratio and minimal end-to-end delay.

CONCLUSION:

The Trust based secure routing is the objective of the proposed route discovery strategy called Explorative Node Eminence State (ENES) Discovery for Secure Routing in Mobile ad hoc Networks. The proposed model is introduced novel node's eminence score assessment and update process. The usual attacks such as eminence tainting, colluding eminence boosting and conditional eminence update are having null impact in ENES. The node divergence in eminence update (see sec 3.2), eminence update frequency (see sec 3.2) and camouflage publishing strategy that used in eminence update (see sec 3.4) are the key features introduced in order to limit the influence of the attacks explored earlier (see sec 3.5). The simulation study (see sec 4.1) and performance analysis (see sec 4.2) evincing that the proposed ENES is scalable and robust that compared to other similar benchmarking model called trust scheme (Y. Khamayseh, 2012). The performance of the ENES was assessed by the traditional metrics called packet delivery ratio, end-to-end delay and process overhead. The model proposed and study conducted in this manuscript can be extended in future to secure the routing from black-hole, gray hole and vampire attacks.

REFERENCES

[1] Abolhasan, M. W. (2004). A review of routing protocols for mobile ad hoc networks. *Ad hoc networks, 2*(1), 1-22.

[2] Arya, S. a. (2012). Malicious nodes detection in mobile ad hoc networks. *Journal of Information and Operations Management*, 210-212.

[3] C. Huang, Y. C. (2007). A Trusted Routing Protocol for Wireless Mobile Ad hoc Networks. *IET Conference on Wireless, Mobile and Sensor Networks* (pp. 406-409). IET.

[4] Carmines, E. G. (1979). *Reliability and validity assessment.* Sage publications.

[5] Conti, M. &. (2014). Mobile ad hoc networking: milestones, challenges, and new research directions. *Communications Magazine, 52*(1), 85-96.

[6] G. Bella, G. C. (2009). Evaluating the device reputation through full observation in MANETs. *Journal of Information in Assured Security* , 458-465.

[7] Woungang, S. D. (2012). Detecting blackhole attacks on DSR-based mobile ad hoc networks. *IEEE Conference.* IEEE.

[8] Issariyakul, T. &. (2011). Introduction to network simulator NS2. *Springer Science & Business Media.*

[9] Mehra, S. K. (2009). Multi-path and message trust-based secure routing in ad hoc networks. *International Conference on Advances in COmputing, Control and Telecom Technologies* (pp. 189-194). IEEE.

[10] P. Michiardi, R. M. (2002). CORE: A Collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. *Advanced communications and multimedia security, Springer*, 107-121.

[11] P. Narula, S. K. (2008). Security in mobile ad-hoc networks using soft encryption and trust based multipath routing. *Computer & communications, ScienceDirect, 31*, 760-769.

[12] Perkins, C. B.-R. (2003). *Ad hoc on-demand distance vector (AODV) routing.* RFC 3561.

[13] Pirzada, A. A. (2007). Dependable dynamic source Routing without a trusted third party. *Journal of Research and Practice in Information Technology*.

[14] Sarwar, B. M. (2001, 02 19). *node16.html*. Retrieved from http://www10.org/: http://www10.org/cdrom/papers/519/node16.html

[15] Shakshuki, E. M. (2013). EAACK—a secure intrusion-detection system for MANETs. *IEEE Transactions on Industrial Electronics*, 1089-1098.

[16] T. Ghosh, N. P. (2004). Collaborative Trust-based Secure Routing Against Colluding Malicious Nodes in Multi-hop Ad Hoc Networks. *29th Annual IEEE International Conference on Local Computer Networks* (pp. 224-231). IEEE.

[17] T. Ghosh., N. P. (2005). Towards Designing a Trusted Routing Solution in Mobile Ad Hoc Networks. *Mobile Networks and Applications, 10*, 985-995.

[18] X. Li, Z. J. (2010). Trust-based on-demand multipath routing in mobile ad hoc networks. *Information Security, IET*, 212-232.

[19] Y. Khamayseh, R. A.-S. (2012). Malicious nodes detection in MANETs: behavioral analysis approach. *Journal of Networking*, 116-125.