http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 11 (8): 980-988, 2012
ISSN 1812-5638 / DOI: 10.3923/itj.2012.980.988

RSA Threshold Signature Based Node Eviction in Vehicular Ad Hoc Network

S.K. Harit, S.K. Saini, N. Tyagi and K.K. Mishra
Motilal Nehru National Institute of Technology, Deptartment of Computer Science and Engineering, Allahabad-211004, Uttar Pradesh, India

Abstract: Vehicular Ad hoc network is a self-organizing net-work between the vehicles that helps in enhancing transportation safety and efficiency. Vehicular Ad hoc network has a wide range of applications that needs a high level of security, as a single vehicle sending out false warnings can disrupt the traffic of whole highway. Eviction of such misbehaving vehicle is a critical issue of vehicular ad hoc network. Almost every approach, proposed for security of vehicular ad hoc network communication is based on public key infrastructure in which only certification authority can revoke the certificate of misbehaving vehicle. In this paper, we propose a node eviction protocol based on RSA Threshold signature which can evict the misbehaving node from vehicular ad hoc network by maintaining the properties of public key infrastructure architecture.

Key words: Vehicular ad hoc network, RSA threshold signature, public key infrastructure

INTRODUCTION

Vehicular Ad hoc network are communication networks formed by vehicles equipped with hardware and firmware components, such as taco-graphs, Event Data Recorders (EDRs) etc. (Pathan, 2010). Initially, vehicular Ad hoc network was designed to provide basis of safe and efficient transportation but later on it was realized that vehicular ad hoc network can be used to offer various services like toll tax payment, safety alerts, congestion warning, location and direction determination of any wanted vehicle by authorities. Vehicular Ad hoc network can also provide additional value added services like, to get information for the shortest (w.r.t. time/distance) path for any desired destination, file transfer between users, accessing Internet, commercial advertisement etc. In vehicular Ad hoc network, there are two modes of communication:

- Vehicle-to-vehicle
- Vehicle-to-infrastructure

Infrastructure mainly consist of road side units, that are located near highways as shown in Fig. 1. It is used for providing the traffic updates, warning signals and for information exchange from certification authority. Dedicated Short Range Communication (IEEE Std. 1609.2-2006, 2006) is used in vehicular ad hoc network for communication between nodes. Vehicular Ad hoc network follow cooperative approach to make network effective in avoiding accidents and traffic congestions. Each node in vehicular ad hoc network is free to disseminate traffic information (Huo *et al*., 2011). But malicious nodes may cause serious security threats in vehicular ad hoc network for e.g., a vehicle can disseminate false information over vehicular ad hoc network intentionally for some selfish reasons to get advantage of traffic condition or for malicious intentions like to design a terrorist attack. Hence, security of vehicular Ad hoc networks is a critical issue for their efficient deployment. Lot of research contributions have been done for securing vehicular ad hoc network from security threats like injection of false data, modification or replay of legitimate information, denial of service, threat to privacy of user's credentials etc. These threats can be avoided by providing security service i.e authentication, verification of data consistency and repudiation of message in vehicular ad hoc network. All proposed security solutions for securing vehicular ad hoc network used public key infrastructure which provides the most suitable security assistance for vehicular ad hoc network infrastructure, for all desired services.

Public key infrastructure (Raya and Hubaux, 2005; AL-Fayoumi and Aboud, 2007) is a public key certificate based scheme. In public key infrastructure, certification authority is a central authority which issues the certificate to the vehicle at the time of registration of vehicle. Each certificate carries user's public key and corresponding private key. These certificates are used for authentication of entities while communicating in vehicular ad hoc network. Certificates are send along with messages in vehicle-to-vehicle communication and validity of

Corresponding Author: Sandeep Kumar Harit, Motilal Nehru National Institute of Technology, Deptartment of Computer Science and Engineering, Allahabad-211004, Uttar Pradesh, India

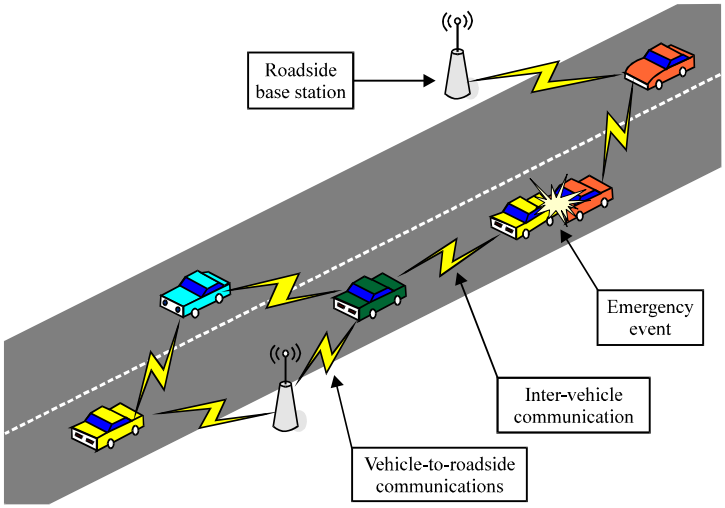

Fig. 1: Schematic representation of a vehicular Ad hoc network

certificate is checked at receiver's end; if certificate found to be invalid then the message is rejected. Sometimes it may happen that certificate is valid but vehicle is deliberately sending false information, these type of vehicle are known as faulty nodes. Certificate of faulty node should be revoked. So, that message from these nodes can be ignored by all other nodes.

In typical approach certificate of vehicle should be revoked only by certification authority and certificate revocation lists (Housley *et al*., 2002) should be disseminated among the vehicles. But this process is time consuming and it is also expected that during initial deployment of vehicular ad hoc network, road side units can not be located everywhere and that will also increase the revocation time. Hence, we need a mechanism for node eviction that should be fast and can protect non-faulty nodes till certification authority revokes certificates of faulty nodes and disseminates certificate revocation list among vehicles, by alerting them about the faulty node's behavior.

In this study, we have proposed a node eviction scheme based on RSA threshold signature (Tang, 2004) with some modification. In proposed scheme, we divided the private key of RSA into N shares (Luo *et al*., 2011) and a set of shares A is computed. Each A_j an subset of set A is delivered to jth vehicle in network. When a misbehaving vehicle is detected any node can start the eviction process by creating the eviction message and then broadcasting this message in order to combine all the partial signatures of to form a complete signature. When complete signature is obtained on the message then message is broad-casted to all the nodes, they will ignore the messages coming from the evicted node. When this message reaches to road side units, it will forward that message to certification authority which will revoke the certificate of that faulty node.

Many researchers have contributed towards the enhancement of vehicular ad hoc network security (Krishna *et al*., 2007). All proposed node eviction schemes (Wasef and Shen, 2009; Raya and Hubaux, 2005; Raya *et al*., 2006) for vehicular ad hoc network focus on two issues revocation of certificate and dissemination of revocation information. When a node shows unusual behavior, neighboring will detect this with help of misbehavior detection system. Misbehavior detection system is used to detect the misbehaving node by monitoring specific parameters of node and data anomalies that do not follow any known pattern. Raya *et al*. (2007) proposed eviction protocol i.e., LEAVE (Local Eviction of Attackers by Detection System) protocol. In LEAVE, when a vehicle detects a malicious vehicle it starts broadcasting warning message. When a vehicle receives this warning message it adds it to accusation list. When sum of accusation for a vehicle exceeds a defined threshold then a disregard message is broad-casted to instruct all the neighboring vehicle to ignore the messages from that misbehaving vehicle. Although the scheme is fine but in this scheme neighboring nodes vote for revocation process which require a majority of honest neighboring nodes. Wasef and Shen (2009) proposed a Decentralized Revocation protocol known as EDR (Efficient Decentralized Revocation protocol). Which revokes the vehicle with help of a group of vehicles. Vehicles vote to revoke the vehicle; votes are collected by revocation coordinator. Revocation coordinator creates a revocation

message and try to collect the revocation share of all the neighboring vehicles. Later on when all revocation shares are collected it computes total revocation message signature. This revocation message is again broadcasted (Zhou *et al*., 2010). Scheme is fine but it is putting a extra overhead on all nodes to send message back to revocation coordinator and then revocation coordinator aggregates those shares to compute revocation message. why not all nodes aggregate there shares? Centralizes aggregation is not effective in a dynamic topology like vehicular ad hoc network where neighborhood keeps on changing all the time. Scheme is very complex and time consuming, for initial deployment we need a simple and fast scheme.

We are proposing an eviction scheme which is very simple and fast enough to evict the faulty node. Our scheme uses threshold RSA signature which is based on a simple secret sharing algorithm. Tang (2004) proposed threshold RSA signature scheme which consist of four stages Shadow (Zhao *et al*., 2010) generation stage, shadow distribution stage, generation of partial signatures and aggregation of partial signatures. We have modified the partial signature generation and combination stages of the scheme to make it compatible with vehicular ad hoc network environment. In shadow distribution stage (Luo *et al*., 2010), only difference is that shadow set may be distribute randomly instead of sequentially. In aggregation of partial signature phase, Tang's scheme require any K participants out of N to reconstruct the secret but any M-1 or less than M-1 than M-1 participants would not able recover the secret where M is:

$$M = \left\lceil \frac{N}{N-k+1} \right\rceil \quad (1)$$

But it will lead to serious problem in vehicular ad hoc network scenario, as it requires k>N/2 for M to be greater than 2. That means, scheme requires at least half of the participants to participate for M>2. Otherwise, only two vehicle can collide to evict the node easily for e.g. Putting N = 1000, K = 499 in Eq. 1 we get:

$$M = \left\lceil \frac{1000}{1000-499+1} \right\rceil$$

$$= 2 \text{ (aprox)}$$

So, instead of K based signature aggregation we apply M based aggregation of signature i.e., making M sufficiently large and keeping K close to N for vehicular ad hoc network which generally has large number of vehicles.

PROPOSED EVICTION PROTOCOL

The proposed protocol is based on Threshold RSA Signatures (Tang, 2004). Proposed protocol consist of two phase distribution of secret key (Du *et al*., 2009) shares and eviction process of faulty nodes.

Distribution of secret key shares: A central certification authority is the only entity in network which issues an authentic digital certificate and the secret key shares for the vehicles in the network (Pathan, 2010).

Certification authority chooses two large prime numbers of equal length (assume 512 bit) p and q at random, where, p = 2 p+1, q = 2 q+1, where p and q are also prime (Shoup, 2000). Compute RSA (Pazynyuk *et al*., 2008) modulus N = p q and n = (p-1)*(q-1). Now, certification authority chooses the RSA (Mousa, 2005) public exponent e such that gcd (e, ϕ(n)) = 1 then certification authority computes d = e^{-1} mod ϕ (n). Denote the public key by (n, e) and private key by (d,n).

Suppose there are N number of vehicles in the network i.e., V_0, V_1, V_2.....V_{N-1}. Randomly select (N-2) numbers:

Symbol table

A_j	Set of shares
B_j	A N-bit vector
H( )	Hash function
PSS	Partial signature set
X	Sum of shares
C	Computed signature
T_{stamp}	Time stamp
|	OR operation
$\oplus$	XOR operation
$\|\|$	Concatenation

A $\{d_0, d_1, d_2.....d_{N-2}\} \epsilon \phi$ (n) then compute:

$$d_{N-1} = d - \sum_{i=0}^{N} d_i \quad (2)$$

Now, compute set A_j where, j = 0, 1, 2,....., N-1. A_j consist of a set of d-shares allocated to vehicle V_j. Each vehicle will have N-k+1 values in its A_j set where k is a positive integer. Set A_j will be distributed among the vehicles as:

$$A_j = (j, d_{i \bmod N}),\ j \le i \le N-k+j \quad (3)$$

where, j = 0, 1, 2,....., N-1 and $d_{i \bmod N}$ is computed using (2).

After receiving A_j calculated using (3), each vehicle will compute a N-bit vector B_j which represent the set of shares vehicle having in set A_j i.e., value from index j to index j+N-k will be set to 1 otherwise 0. After this phase each vehicle in vehicular ad hoc network will have:

- Set of shares A_j
- A N-bit vector B_j
- A short-life certificate with public key of vehicle
- The hash fuction H( )

Eviction process of faulty node: When a misbehaving vehicle is detected then its neighbor will start the eviction process by using algorithm 1.

Eviction steps:

- Suppose V_s started the eviction process. V_s will create a N-bit vector whose all bit are set to 0 and name it as say Partial Signature Set (PSS). Basically, partial signature set is used to keep track aggregated of shares i.e. out of N shares how many shares are aggregated? When all the bits in partial signature set will be 1, it implies that all the shares has been aggregated and eviction message may be generated

    - V_s takes all of it's shares from A_s and compute:

$$X_S = \sum_{i=S}^{S+N-k} d_i \bmod n \quad (4)$$

where X_s denotes the sum of shares of node V_s.

- V_s will create a message 'm' attaching the certificate of misbehaving vehicle and reason of eviction of the vehicle
- C_s will compute its signature:

$$C_s = (H(m))^{x}s \bmod n \quad (5)$$

C_s is computed signature generated by V_s after integrating it's secret shares X_s from (4).

- Now, V_s will update partial signature set vector by:

$$PSS = PSS\ (OR)\ B_s$$

Partial signature set updation is required to inform other nodes that all those bits that are set 1 in partial signature set, those shares have been already integrated. So, When any other node will check the partial signature set bits then that node will not integrated those shares whose bit is set to 1 in partial signature set.

- V_s broadcasts a request message:

$$m \parallel C_s \parallel PSS \parallel T_{stamp}$$

This request message will contain message m generated by V_s along with computed signature (Aboud and AL-Fayoumi, 2007) C_s using (5), updated PSS and current time stamp T_{stamp} of the vehicle.

Algorithm 1: Algorithm for the initiator node V_s

Require: A message $m = Cert_{mb} \parallel Reason \parallel T_{stamp}$

Ensure:

1: PSS ← [0000... Upto N bits]

2: $X_S \leftarrow \sum_{i=S}^{S+N-k} d_i \bmod n$

3: $C_S \leftarrow (H(m))^{X_s} \bmod n$

4: PSS←PSS| B_s

5: $M \leftarrow m \parallel C_s \parallel PSS \parallel T_{stamp}$

6: return M

- Any vehicle receiving the request message. Checks the validity of time stamp T_{stamp} by checking ($T_{current}$-$T_{received}$) <= δ T, where, $T_{current}$ denotes the vehicle current time stamp and δ T is permissible time interval for transmission delay. If request message is received within permissible transmission delay then V_j will use algorithm 2 for evicting the misbehaving vehicle

    - Vehicle V_j will check the vector PSS. If all the bits are set to 1 then eviction message group signature i.e.

$C = (H(m))^d \bmod n$ is generated which can be verified using public key of Certification Authority. Hence, certificate eviction message $m \parallel C \parallel T_{stamp}$ has been completed.

- Otherwise compute:

$$E_j = PSS \oplus B_j$$

When partial signature set is XORed with B_j we get E_j. All those bits in E_j that are set to 1 will represent d shares which V_j have but still not used in partial signature set.

- V_j compute sum of all those d_i share i.e.:

X_j = {Sum of all d share chosen using E_j} mod n

where, X_j denotes the sum of shares of node V_j. (d) V_j compute:

$$C_j = (C_s)^{X_j} \bmod n \quad (6)$$

C_j is computed signature generated by V_j after integrating it's secret shares to received signature C_s.

- Then V_j will update the partial signature set by:

$$PSS = PSS\ (OR)\ B_j$$

Now, again partial signature set updation is required to inform other nodes that node V_j has integrated it's shares to partial signature set.

- V_j broadcasts a request message:

$$m \| C_s \| PSS \| T_{stamp}$$

This request message will contain message m generated by V_s along with computed signature C_j using (6), updated partial signature set and current time stamp T_{stamp} of the vehicle.

Algorithm 2: Algorithm for the other node V_j

Require: A message $M = m \| C_s \| PSS \| T_{stamp}$
Ensure:
1: if PSS = = [11111...up to N bits] then
2: $C_s \leftarrow (H(m))^d \bmod n$
3: $REV_{msg} \leftarrow m \| C \| T_{stamp}$
4: Complete REV_{msg} generated
5: else
6: $E_j \leftarrow PSS \oplus B_j$
7: $X_j \leftarrow$ {Sum of all d shares chosen using E_j} mod n
8: $C_s \leftarrow (H(m))^{X_j} \bmod n$
9: $PSS \leftarrow PSS|B_s$
10: $M \leftarrow m \| C_s \| PSS \| T_{stamp}$
11: broadcast M
12: end if

After the completion above of process, eviction message (REV_{msg}) is broad-casted in the neighborhood of evicted vehicle. All the vehicles in neighborhood of evicted vehicle will ignore the messages from the evicted vehicle. When this message will be captured by road side units, it will check the message validity and then forward the message to certification authority. Then the certification authority will revoke the evicted vehicle's certificate and then add the certificate of revoked vehicle into certificate revocation list. This certificate revocation list contains certificates which are revoked but yet not expired. Then certificate revocation list is disseminated to every vehicle present in the vehicular ad hoc network.

PERFORMANCE ANALYSIS

Here, we have carried out performance analysis of our scheme in terms of computation, probability of eviction, decentralization of eviction process etc.

Decentralized eviction process: Our eviction scheme is decentralized scheme as aggregation of shares is performed by the nodes where as in other schemes like EDR aggregation of revocation shares is performed by revocation coordinator. EDR pretends to be decentralized. But uses of revocation coordinator for aggregation make this scheme centralized. In EDR as shown in Fig. 2, Vehicle A detects a misbehaving vehicle B. Now, vehicles A acts as revocation coordinator and creates a revocation request message. Vehicle A will broadcasts revocation request message to all one-hop neighboring vehicles. All vehicles i.e., C, D, E, F, G, H, I, J will send their revocation shares back to Revocation Coordinator (Vehicle A). Then vehicle A aggregates all the received shares to form a revocation message. But this will increase the overhead on the network and will double the number of broadcasts required for evicting a Vehicle as all node sending revocation shares back to revocation coordinator. EDR assumes that all neighborhood vehicles will send their revocation shares but as neighborhood is dynamic in vehicular Ad hoc network, it could happen that those vehicles who have received the revocation request are no more in neighborhood of revocation coordinator because of their high or low speeds. In EDR, revocation is performed on basis of one-hop neighboring vehicles only it implies EDR ignore the opinion of all other vehicles. But in proposed scheme as shown in Fig. 3, when a vehicle A detects misbehaving vehicle B then vehicle A creates an eviction message and add its share to this message, then broadcasts this message with updated partial signature set. Similarly, all other vehicles receiving this message will add their shares to this message and re-broadcasts it with updated partial signature set. When complete signature generated, all vehicles receiving eviction message will ignore the message coming from vehicle B. Our scheme works at larger scale, a large group of vehicles will be taken in confidence before any eviction from vehicular Ad hoc network.

Threshold based eviction: In EDR, revocation coordinator broadcasts a request to provide their revocation share to all one-hop neighboring vehicles. Any neighboring vehicle receiving revocation request will broadcasts its revocation share. When revocation coordinator gets revocation shares, he calculates final revocation message and broadcasts this message to all neighboring vehicles. But what if there are very less number of neighbors in neighborhood? secondly, as we know that speed of vehicles changes frequently in vehicular ad hoc network this implies that neighborhood will also change frequently. So, one should also concern other vehicles that came in contact with misbehaving vehicle 5-10 min before. In our scheme, we have defined a threshold M i.e., at least M vehicle's d shares would be required to revoke a vehicle where M varies with number of vehicles in vehicular Ad hoc network.

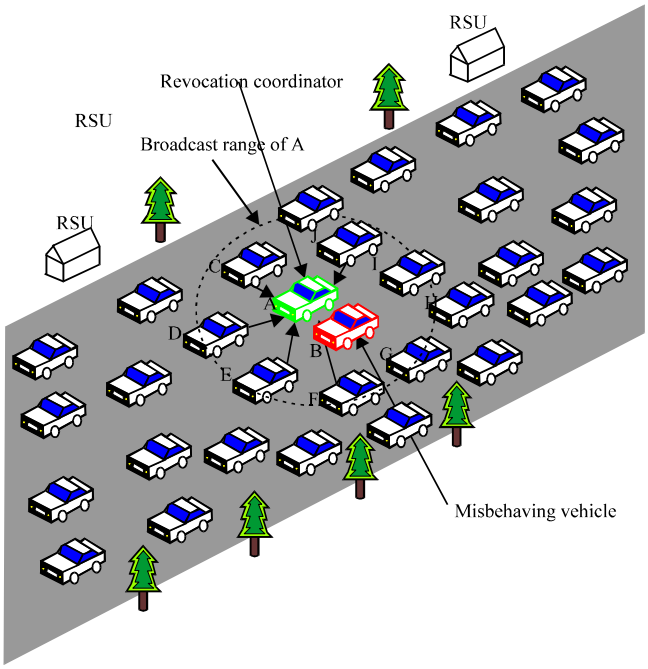

Fig. 2: EDR mechanism to revoke misbehaving vehicle in vehicular Ad hoc network

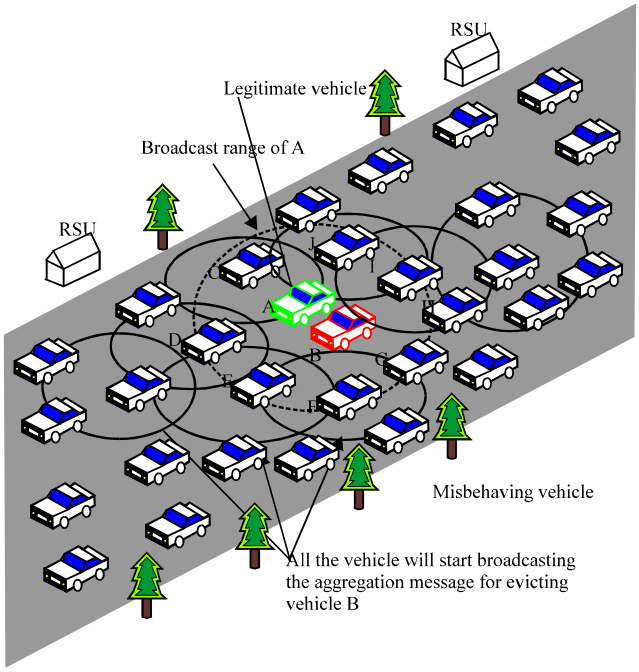

Fig. 3: Par posed scheme mechanism to evict a misbehaving vehicle in vehicular Ad hoc network

Dissemination of eviction message: In our scheme the eviction message after completion will spread in vehicular ad hoc network very fast as compare to any other scheme. As we have know in all other scheme the eviction message is generated by one vehicle and only that vehicle may start broadcast of eviction message (Samara *et al*., 2011) in vehicular Ad hoc network. On other hand in our could happen that many vehicle compute same eviction message in different geographical area at same time. So, more than one vehicle may start broadcasting same eviction message in different geographical area.

Probability to evict a vehicle: If Tang's Scheme (Tang, 2004) is directly (without any modification) used in

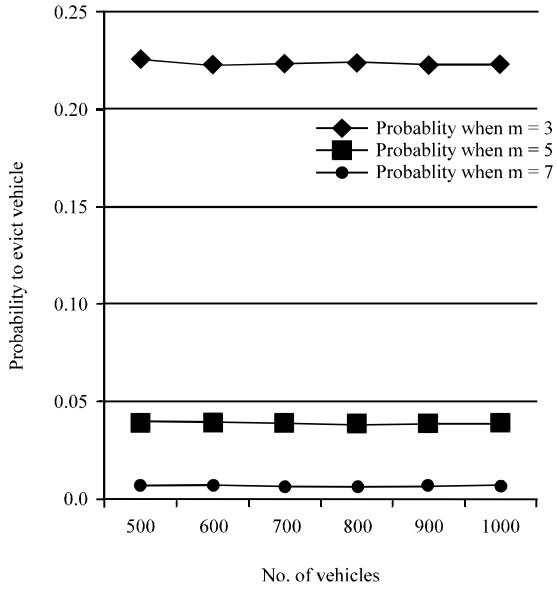

Fig. 4: Probability to evict a vehicle with increase in number of vehicles vehicular Ad hoc network

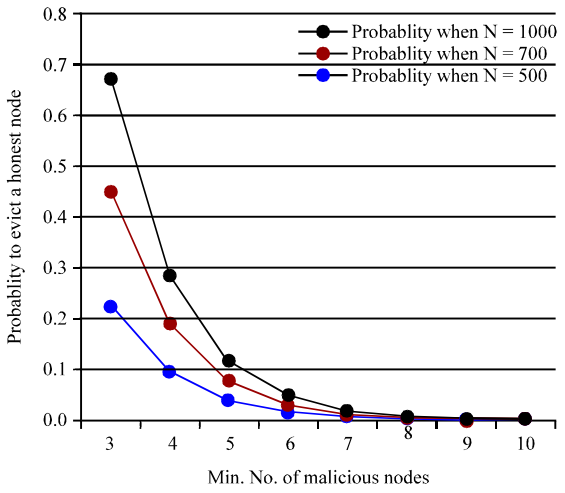

Fig. 5: Probability to evict a vehicle with increase in minimum number of malicious node in vehicular Ad hoc network

vehicular ad hoc network scenario, that will lead to a serious problem in vehicular Ad hoc network. Tang's scheme (Aboud, 2007) requires any K participants out of N to reconstruct the secret but any M-1 or less than M-1 participants would not able recover the secret where M is defined in (1).

It means scheme requires at least half of participants to participate for M>2 as shown in Fig. 4. Otherwise, two vehicles can collide to evict a vehicle easily. That means a group of 2-3 malicious vehicle can evict an honest vehicle.

To prevent honest vehicles, instead of K based signature aggregation we apply M based aggregation signature i.e., keeping K close N will make M sufficiently large. When M will be large than eviction process will require more vehicle shares to evict a vehicle. That means probability to evict a vehicle will be:

$$Pr_{ev} = \prod_{i=1}^{M} \frac{N - i(N - k + 1)}{N - i} \quad (7)$$

So, it means that when N is fixed and we increase K than M will increase that will to decrease in probability to evict a vehicle as shown in Fig. 5.

This will protect honest vehicles from malicious i.e., 2-3 malicious vehicle will not able to revoke an honest vehicle.

Performance optimization: We can optimize our eviction scheme to make scheme more practical, efficient and effective in evicting faulty node from vehicular Ad hoc network. For optimization,

- We are required to minimize the number of broadcasts required for eviction
- Ensure the dissemination of eviction information
- Maximize the aggregation of shares per broadcast

To minimize number of broadcasts required we can apply one condition that a vehicle during aggregation phase will broadcast request message if and only if it has added x% of required shares in partial signature set. The value of x will decided by initiator of message on the basis required number of shares in partial signature set. Suppose a vehicle A has added 20% of shares and but still 80% shares required for completion of eviction message. Vehicle A will apply a condition that next vehicle will broadcast the message if and only if that vehicle will add 5% of required 80% shares. This optimization will reduce number of broadcasts required for aggregation phase. To ensure the dissemination of eviction information for aggregation of shares, each vehicle after broadcasting eviction message will check whether he received any broadcast of eviction message from its neighborhood after his broadcast. If vehicle did not get any broadcast after a predefined time interval then it will again broadcast the same eviction message. This process will be repeated at least 3 times, in case after 3 times vehicle did not get any replied broadcast then process of eviction will be delayed for a time interval.

To maximize the aggregation of shares, we can use duplicate shares i.e., instead of dividing secret into N

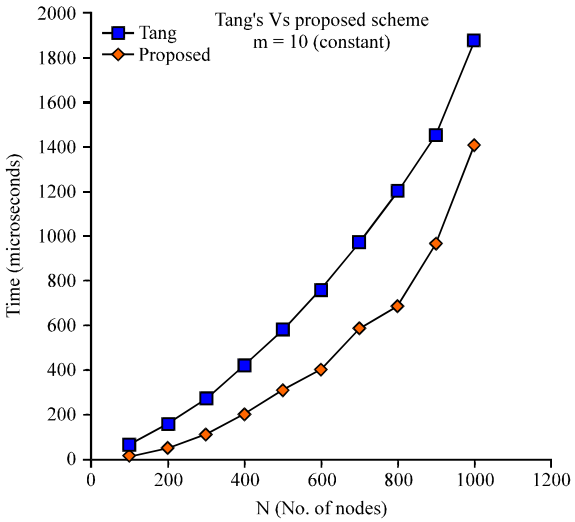

Fig. 6: Comparison of tangs scheme and proposed Scheme when number threshold M is constant

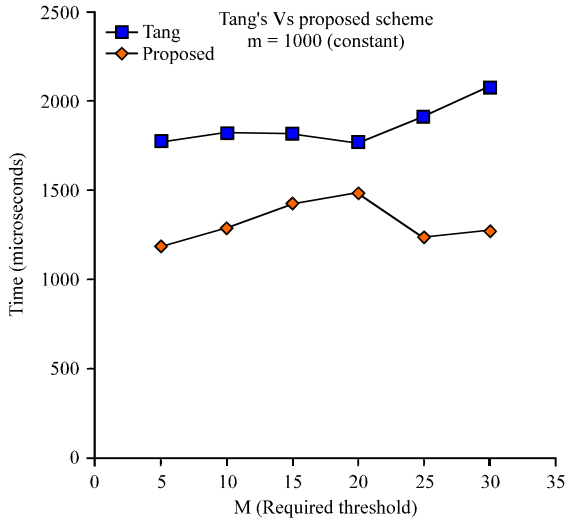

Fig. 7: Comparison of tangs scheme and proposed scheme number of vehicles N is constant

shares; we will divide it into N/2, N/4 shares. This means that if we have divided secret into N/2 shares then half of vehicles in vehicular ad hoc network will have same shares, it will maximize the aggregation of shares.

Computation and storage: Our eviction scheme is very simple and less time consuming. Our scheme uses only simple operations like addition and logic operations where as other proposed schemes uses very complex procedures like EDR uses bilinear pairing and LEAVE uses a complex way to calculate eviction quotient. We plotted two graphs for tangs scheme and our proposed scheme. In one graph we have taken k (threshold constant) as constant and in other graph we have taken n (no of nodes) as constant.

In Fig. 6, we have taken number of nodes (vehicles) in vehicular ad hoc network on X-axis and time taken by schemes on Y-axis. We have taken M (threshold constant) as 10. It is clearly visible that our scheme takes less Computation time in comparison to Tang's scheme.

In Fig. 7, we have taken M (the threshold) in vehicular ad hoc network on X-axis and time taken by schemes on Y-axis. We have taken the number of nodes (N) as 1000. It is clearly visible that our proposed schemes take less Computation time in comparison to Tang's scheme.

CONCLUSION

In this study, we have proposed a node eviction scheme based on RSA threshold signature for vehicular ad hoc network. Our scheme is very simple, fast and less time consuming in comparison to all other proposed node eviction scheme. It is purely decentralized scheme and saves times in term of eviction in-formation dissemination among the vehicles. We also pointed out limitation of our scheme and presented a solution to overcome that limitation. In our scheme there is scope for future work and we are trying to make scheme more practical, efficient and effective in evicting faulty node from vehicular Ad hoc network. Our future work will focus on simulation of proposed scheme and experimenting it in real vehicular ad hoc network condition.

ACKNOWLEDGMENT

We would like to thank all reviewers in advance for their valuable suggestion to improve the study.

REFERENCES

Aboud, S.J. and M.A. Al-Fayoumi, 2007. A new multisignature scheme using re-encryption technique. J. Applied Sci., 7: 1813-1817.

Aboud, S.J., 2007. Efficient scheme for obtaining public key cryptosystem using shared secrets. Inform. Technol. J., 6: 259-262.

Al-Fayoumi, M.A. and S.J. Aboud, 2007. Identity authentication and key agreement schemes for ad hoc networks. J. Applied Sci., 7: 1638-1642.

Du, C.L., M.Z. Hu, H.L. Zhang and W.Z. Zhang, 2009. Anti-collusive self-healing key distribution scheme with revocation capability. Inform. Technol. J., 8: 619-624.

Housley, R., W. Polk, W. Ford and D. Solo, 2002. Internet X.509 public key infrastructure certificate and Certificate Revocation List (CRL) Profile. RFC 3280, http://www.ietf.org/rfc/rfc3280.txt

Huo, M., Z. Zheng, X. Zhou and J. Ying, 2011. PCAR: A packet-delivery conditions aware routing algorithm for vanet networks. Inform. Technol. J., 10: 1334-1342.

IEEE Std. 1609.2-2006, 2006. IEEE trial-use standard for wireless access in vehicular environments security services for applications and management messages. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1653011

Krishna, B.A., S. Radha and K.C.K. Reddy, 2007. Data security in ad hoc networks using randomization of cryptographic algorithms. J. Applied Sci., 7: 4007-4012.

Luo, H., F.X. Yu, H. Li and Z.L. Huang, 2010. Color image encryption based on secret sharing and iterations. Inform. Technol. J., 9: 446-452.

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inform. Technol. J., 10: 681-685.

Mousa, A., 2005. Sensitivity of changing the RSA parameters on the complexity and performance of the algorithm. J. Applied Sci., 5: 60-63.

Pathan, A.S.K., 2010. Security of Self-Organizing Networks: MANET, WSN, WMN, VANET. Auerbach Publications, USA.

Pazynyuk, T., G.S. Oreku and J. Li, 2008. Distributed Signature Scheme (DSS) based on RSA. Inform. Technol. J., 7: 802-807.

Raya, M. and J.P. Hubaux, 2005. The security of vehicular ad hoc networks. Proceedings of the 3rd ACM Workshop on Security of ad hoc and Sensor Networks, November, 2005, Alexandria, USA., pp: 259-262.

Raya, M., D. Jungels, P. Papadimitratos, I. Aad and J.P. Hubaux, 2006. Certificate revocation in vehicular networks. Technical Report LCA-Report- 2006-006, 2006 Swiss Federal Institute of Technology in Lausanne, Lausanne, Switzerland.

Raya, M., P. Papadimitratos, I. Aad, D. Jungels and J.P. Hubaux, 2007. Eviction of misbehaving and faulty nodes in vehicular networks. IEEE J. Sel. Areas Commun., 25: 1557-1568.

Samara, G., W.A.H.A. Alsalihy and S. Ramadass, 2011. Increase emergency message reception in vanet. J. Applied Sci., 11: 2606-2612.

Shoup, V., 2000. Practical threshold signatures. Adv. Cryptol., 1807: 207-220.

Tang, S., 2004. Simple secret sharing and threshold RSA signature scheme. J. Inform. Comput. Sci., 1: 259-262.

Wasef, A. and X. Shen, 2009. EDR: Efficient decentralized revocation protocol for vehicular Ad Hoc networks. IEEE Trans. Veh. Technol., 58: 5214-5224.

Zhao, Z., H. Luo and Z.M. Lu, 2010. Shadow size reduction and multiple image secret sharing based on discrete fractional random transform. Inform. Technol. J., 9: 298-304.

Zhou, L., G. Cui, H. Liu, D. Luo and Z. Wu, 2010. NPPB: A broadcast scheme in dense VANETs. Inform. Technol. J., 9: 247-256.