A Clique based Adaptive Intrusion Detection Approach to Provide Trust on Secured Mulicast Group Communications over Manet – Skema

S. Saravanan
Assistant Professor,
Department of Computer Science & Engineering,
Annamalai University
Annamalainagar – 608 002,
Tamil Nadu, India

R M. Chandrasekaran
Professor
Department of Computer Science & Engineering,
Annamalai University
Annamalainagar – 608 002,
Tamil Nadu, India

ABSTRACT
Though numerous research challenges in security focus on MANET, the need for design based secure Group Communication Systems (GCSs) is always a major constraint. The constraint is felt towards incorporation of group based multi-hop security for variable services which requires resource constraints. SKEMA adopts Clique based graph theoretic approach to detect node activity and identifying neighbors during random mobility. SKEMA focuses on towards design of trust mapping mechanism by identifying the maximal connectivity in network. SKEMA also works on developing a random key based exchange approach among clustered nodes in network. SKEMA has been tested over CLIQUES and PROFIDES schemes over secured session maintenance and handling node failure. SKEMA performs better when compared with existing approaches and hence suits well for multi-hop type of services.

Keywords
Secure group communication systems, MANET security, Clique approach, ns2 simulator, SKEMA

1. INTRODUCTION
Numerous research works [1] [10] [14] towards providing security for MANET has been discussed and surveyed over the past decades. The need for a simple and effective trust based evaluation procedure for large and dynamic nodes on mobility is always on high demand. As MANET follows dynamic and random mobility, establishing a secured communication is always a challenge. This paper discusses on the following objectives

(a) to design trust mapping mechanism over secured MANET by identifying the maximal connectivity in network.

(b) To develop a random key based exchange approach among clustered nodes in network.

An adaptive trust based security in MANET demands high complexity which involves node mobility pattern, user profile organization, and traffic intensity over service in use, node intensity and session being established. In MANET, node self-organization, decentralization and openness are its advantages, which introduces insecurity[9]. MANET nodes do move in consistent mobility in all directions randomly. Nodes join or leave the network, hence the network does not maintain any centralized authority. It can be understood that such nodes lack insufficient information about each other, hence increases the risk of being compromised or being attacked by malicious users.

Numerous technical challenges need to be involved in the design of secure Group Communication Systems (GCSs) in MANET, few issues being faced for implementation includes resource-constrained environments [5] (e.g., bandwidth, memory size, battery life, and computational power), eavesdropping [14] and security threats[24], unreliable communication, no infrastructure support, and dynamic changes in network topology due to user mobility. It also be noted that traditional schemes suffer from risky management and safe keeping of a small number of private and public keys [3] [6].

This paper proposes a secured group key based algorithm SKEMA, which enforces an adaptive security approach among multiple nodes in network. The work also supports on design of efficient and low cost based key management architecture for multicast communications over minimal resource constrained, infrastructure less and dynamic environment. SKEMA is implemented using maximal connectivity vertices of graph G, which are defined as sub-graph K, where nodes in $K \subset G$, it is defined as a Clique. Clique graph helps to resolve the complexity of securing nodes in MANET graph G.

This paper uses Clique based graph theoretic approach to detect node activity during random mobility. Any node can take the responsibility of being the "forwarder node" between the source and destination. The nodes work on token enabled key assignment approach, which generates simple tokens which are assigned as key to a node for a random time interval 'tta'. SKEMA supports through minimal computational overhead complexity which can be largely reduced, as well improves the trustworthiness of routing procedure can be guaranteed as well.

The contributions of SKEMA scheme can be summarized as follows:

(a) Design of group or cluster based asymmetric key exchange over on multicast sessions enabled for communication.

(b) Definition and incorporation of Clique graph in network is suggested for active nodes, hence minimizing the processing time and execution time.

The paper is organized as Sections, where section-1 focuses on detailed introduction to MANET, its need for security and

methods where Clique based graph technique can support towards providing security to active nodes which act as a source or destination node or as forwarding nodes towards data transmission. Section-2 provides detailed review on key based exchange techniques and gaps in research work for SKEMA. Architecture and functionality of SKEMA is discussed in section-3 with detailed algorithms. Section-4 elaborates on experimental test-bed using ns2 simulator [12], while the performance of SKEMA is discussed in Section-5. Section-6 summarizes SKEMA with need for future work.

2. RELATED WORK

Due to insecured network setup, following issues are encountered such as Confidentiality [16], Authenticity, Integrity, Availability, Non-repudiation and Access control establishing a communication setup on MANET is always a challenge. The challenge involves in secured data transfer and information mishandled by untrusty members on channel. Securing data on communication path can be implemented using a cryptographic technique. But securing session on transmission needs key exchange mechanism where members who understand each other on an acceptable end share keys and transmit data.

2.1 Security in group communication

Recent interesting research works have been carried out on group key agreement by Saminathan et al[18] and George Theodorakopoulos et al. [7]. Almost all group key agreement protocols can be directly adapted to conference key agreement. However, most of them operate only when all conferees are honest but do not work when some conferees are malicious and attempts to delay (or) destruct the conference. Sometimes the conferees may cause severe damage to the conference setup or break the session in use.

The unique operational environment of MANET nodes prefers communication medium being open to hackers and eavesdroppers. Such threats increase the need for securing and safe guarding the communication network. Open networks such as MANET, WSN, which need to work on open public environments requires adequate key management protocols support to mitigate the damage caused. Even though th numerous research works had worked on group-key protocols to secure both inter and intra network communication, but still the reviews suggest that neither the issue of the size of a group nor its geographic boundaries are addressed. Much of recent research studies [2],[8],[13] indicate that application of trust model into MANET system along with key based management may lead to much concrete and applicable designs proposed for the security of routing protocols of MANET [11]. This leads to applications such as reputation based monitoring systems [15], where malicious users do pollute the reputation values by issues such as false-praising [25] other collaborating malicious nodes and hindered policy management tasks.

Many security schemes from different aspects of MANET have been proposed in order to protect the routing information or data packets during communication over secure routing protocols [7],[13],[20],[27] and secure key management solutions [13],[19]. Based on literature studies such as PROFIDES [18], and CLIQUE [15] supports security provisioning based on pairwise-key protocols using asymmetric keys which can overcome the drawback of group-key protocols, which are highly restrictive and impose substantial storage overhead on resource constrained MANET nodes[22]. They do not suit the reputation monitoring systems either, since messages encrypted with pairwise-keys render promiscuous monitoring systems being useless.

2.2 Analysis of Key Exchange Approaches

Asymmetric keys uses two parts key, where each recipient has a private key that is kept secret and a public key that is published for everyone. Bing Wu et al [4] adopts the responsibility of generating the partial certificates and storing the certificates in directory structure through which mobile nodes can request for the certificates of other mobile nodes. URSA is a localized key management scheme proposed by Hoeper and Gong [4]. URSA is efficient and provides reliable availability with having the features of encrypted local communication. This model uses efficient threshold scheme to broadcast the certificate (RSA certificate) signing keys to all mobile nodes. This scheme generates communication delay, search failure and degrades the system security. To protect the network from DOS attack and the compromise the signing key URSA using verifiable and proactive secret sharing mechanisms. The advantage of this scheme is efficiency and secrecy of local communication, as well as system availability since the CA's functionality is distributed to all network nodes. On the other hand, it reduces system security, especially when nodes are not well-protected because an attack can easily locate a secret holder without much searching and identifying effort.

Yun Teng et al [25] proposed Mobile Certificate Authority (MOCA), where the mobile nodes which possess high computational power, physically more secure and on the basics of heterogeneity those mobile nodes used as MOCA nodes in this asymmetric scheme. Weimerskirch [23] proposed Self-Organized Key Management (SOKM) model which uses two local certificate repositories where one is updated and another one is non-updated certificate repository. Wu et al adopts Secure and Efficient Key Management (SEKM) [22] which is only asymmetric key management scheme (based upon virtual CA trust model), Safe procedure for interacting, coordination between secret shareholders and efficient that have more responsibility. This model uses mesh structure for server group.

3. DEFINITIONS AND MODELING APPROACH

MANET networks are formed by grouping tiny, self-organized, autonomously running and generally radio-communicable and smart sensor devices into a network in some specific geographical region. Distributed route support algorithms permit route discovery and node management which provide nodes to communicate and generate messages to carry data to other nodes and /or to specific domains in networks. To establish secure communication among MANET nodes the need to provide an efficient authentication and certification services is the primary objective of this work.

3.1 Definitons

The MANET can be modeled as an undirected graph G=(V,E) where V is the set of vertices and E is the set of edges interconnected. Group of nodes involved in communication can establish the session. To provide security among nodes engaged in communication, random key based security might not be an optimal solution, hence incorporating group security among nodes over variable service based on node policy and session in use are the major parameters which devise an optimal security over adhoc networks [26]. Interconnecting multiple nodes over the network for a controlled session needs consistent bandwidth to provide QoS with support over

secured route management for variable users who join into network and leave from network or session in establishment.

A Clique in graph G(V,E) consists of subset V' of V, where v belongs to V', hence there exists a common edge between v and other vertices V'. Identifying maximal cliques with clustering is proposed in Saminathan et al [19] and [21] which does not follow any cluster head.

SKEMA can be envisaged as a network with N MANET nodes, where each node is randomly assigned a unique ID prior to its deployment. The test bed deployment assumes that the nodes are benign for a time period ± t during which every node ni broadcasts its identity and degree of information over its neighborhood 'nj'.

3.1.1 Cluster and Clique Definitions

A graph G(V,E) is a collection of nodes 'ni', where i={1,2,…n} forming clusters C1, C2.. Cn such that all neighboring nodes engaged in a disjoint set forms a cluster C. The size of a cluster depends on number of active nodes involved in session establishment in cluster C. 'n' being the number of nodes involved in a session, hence size k is 'n'. The reachability of nodes between the source and destination depends on the number of hops involved in establishing a session. Fig. 1 shows nodes ni, where i= {a,b,…o} which are involved in establishing path for communication.

A node is defined as a member of graph G, which can be member of Clique graph K, iff it follows the property of Clique in a graph G. The node ni can belong to cluster C, iff the node 'ni' involved in communication can act as member of route to be established.

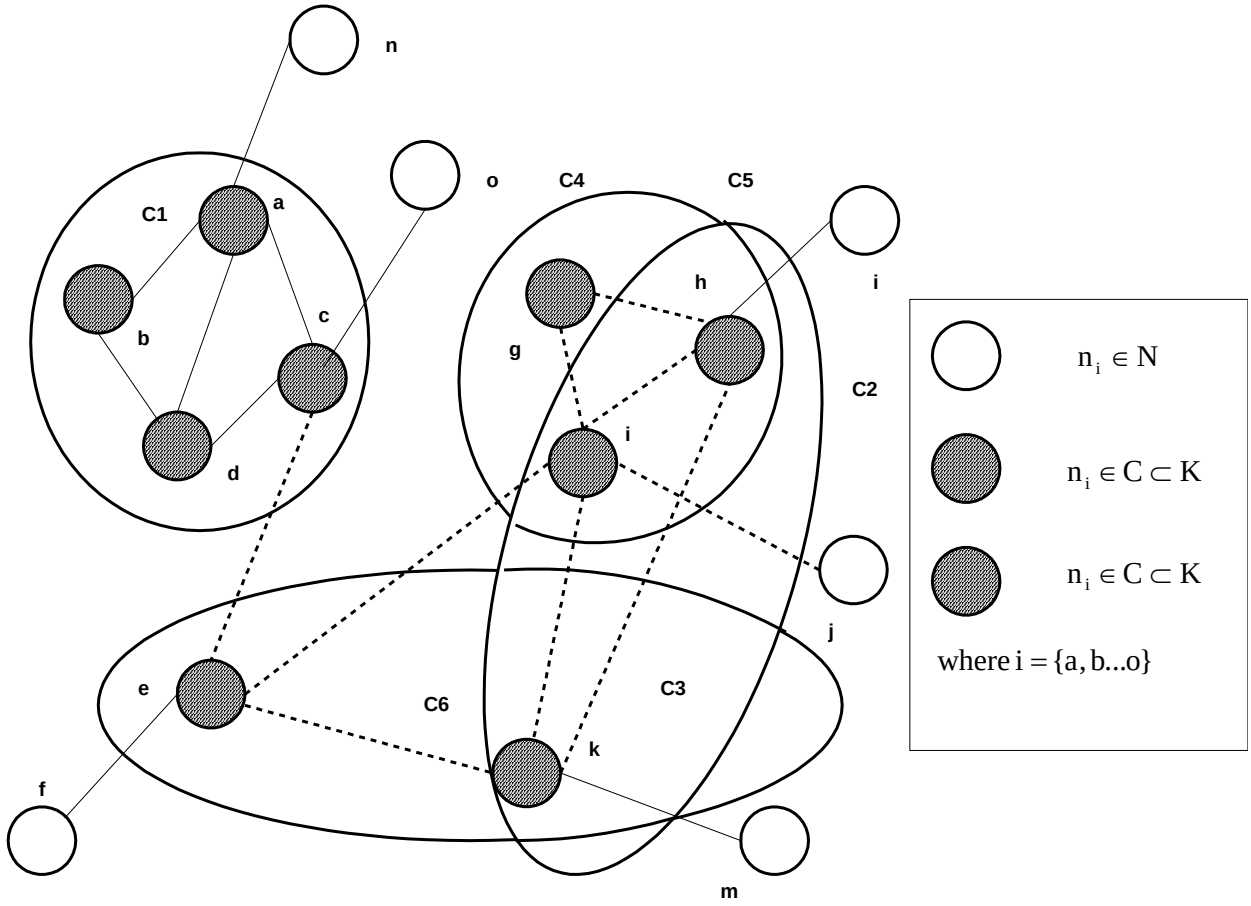

Fig 1: MANET Nodes with Maximal Clique and Clustered

3.1.2 SKEMA adopts the following definitions to support adaptiveness among secured nodes

a. Any MANET node ni ∈ Ci cluster, iff when ni ⊂ G, where G (V,E) is a graph, which consists of all nodes, where i = {1,2,…n}

   The set of nodes 'ni' in network N forms a graph N, as well the same node can also be part of cluster Ci, where cluster Ci can be considered as subgraph of N as shown in Fig. 1.

b. Any new node nk, entering into the secured network N should be assigned a new trust value Tv iff, nk ∈Ci, while Ci ⊂ N, and ∀ ni possess Trust Value Tv[ni] over network.

   New node entering into network N or cluster Ci, should be assigned a new Trust Value Tv based on its service profile in use, node type, such that when the node moves out of network or cluster the Tv gets expired.

c. Any node nk, leaving the trusty network, updates its Trust Value Tv with all other nodes in subnet, such that all nodes should re-initiates its Trust Value Tv.

   The trust value Tv of node should be re-initiated or re-generated at random time intervals or when it leaves its sub net.

d. All nodes 'ni' in a clique graph Ci belongs to Cluster Ki should be recognized as part of graph G.

A node 'ni' being part of defined cluster Ci may participate in communication iff when node belongs to Clique graph Ki, since the node possess the Trust Value property Tv along with its secured key property Tc or Tk.

As shown in Fig. 1, node 'ni' where i = {c,e,i,k } are clique marked nodes, while C1 = {a,b,c, d} being member nodes of cluster C1 which also includes clique node 'c'. Non active nodes are defined as nz ={n,o,f,m,j,i}, while all other nodes of set G are considered as active nodes, which participate in transmission of secured data between source and destination.

4. ARCHITECTURE – SKEMA

To handle multiple attacks from intruders and eaves dropping, members authentication, integrity of data, multi-key exchange management protocol has to be adopted. The Key Management Protocol takes the responsibility of key generation [17] and distribution of distributed cluster [20] managed key protocol over multiple nodes.

SKEMA adopts the following definitions:

N – Nodes in network as graph G (V,E)

ni – Any node in network N, where i = {1,2……n}

Ci – Cluster of nodes or group of nodes

Ki – Nodes which are marked in Clique graph used as forwarding nodes. Ki $\in$ Ci and Ki $\subset$ N

tta – Time To be Alive for assigned or exchanged key Tv

Tv – Trust Value of node 'ni'

Tc - Trust Value of Cluster 'Ci'

Tk – Trust Value of marked Clique node 'Ki'

SKEMA based architecture [Fig. 2] supports in providing multiple session security over MANET network handling various type of services. SKEMA architecture as shown in Fig-2 works on MANET nodes being clustered based on type of service and neighborhood node on mobility.

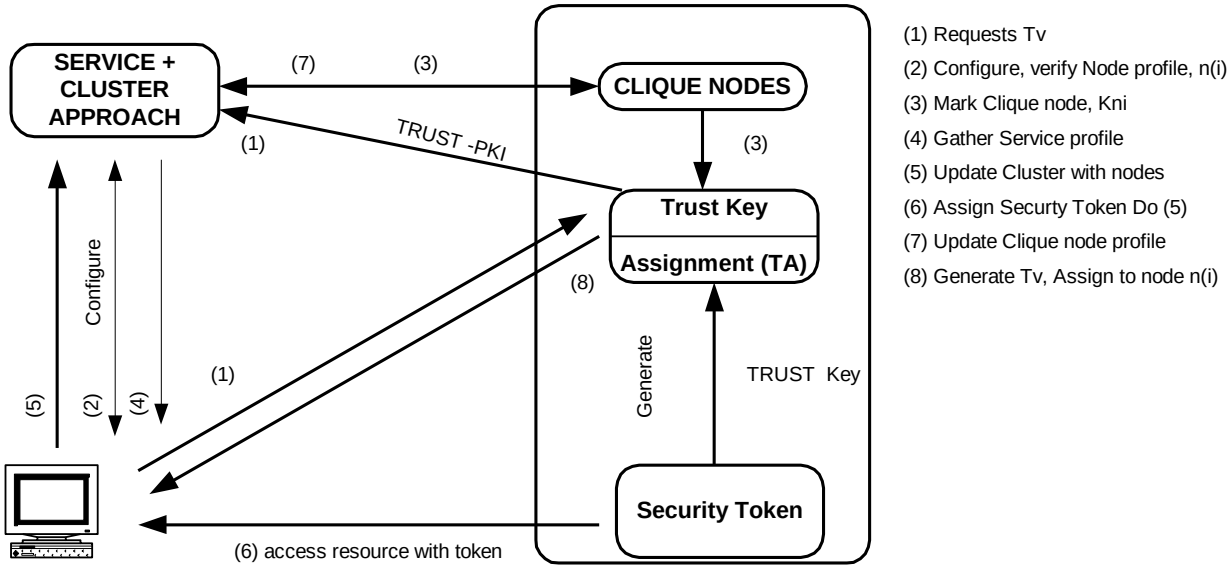

Fig 2: SKEMA Architecture and Functionality

SKEMA scheme, adopts clique graph phenomenon [10], where nodes are located based on their mobility and location. Fig. 1 indicates node 'ni' as Clique node which should be present in a cluster Ci, where cluster Ci should possess atleast one clique node. The clique nodes are ear-marked with pair-wise key generated as (Tc, Tk), where Tk is the unique generated trust value key assigned to node 'ni', which are recognized as forwarding nodes. Tc is the trust value assigned to node 'ni' which is within the cluster but cannot be the clique node.

SKEMA suggests the mechanism of providing Trust Value Tv for a node 'ni' only when the node is confirmed to provide an active role in transmission of data between the source and destination. All nodes other than 'ni' which are not part of cluster Ci or clique graph Ki can be termed as 'no' such that no = ϕ, hence neglected in SKEMA process.

4.1 Skema Functionality

Nodes or members involved in communication establish an cluster or group [5] based intra-path setup among other secured nodes on mobility over defined public or private channel. Each member node ni establishes a communication path only if node nj possess the secured key.

The functionality of SKEMA [Fig. 3] involves embedding a secured key to the node 'ni' which is involved in communication. When a node 'ni' is defined as member or group of cluster Ci, it possess a key Tv[ni] such that the key is valid or maintained until the node is member of cluster Ci as per section 3.1.2[C]. When a node moves out of the cluster Ci, node is expected to refresh its key as the time 'tta' $\leq$ 1ms. Algorithm 1 explains the definition of Tv (Trust Value) and assignment for the nodes as per section 3.1.2 [B]

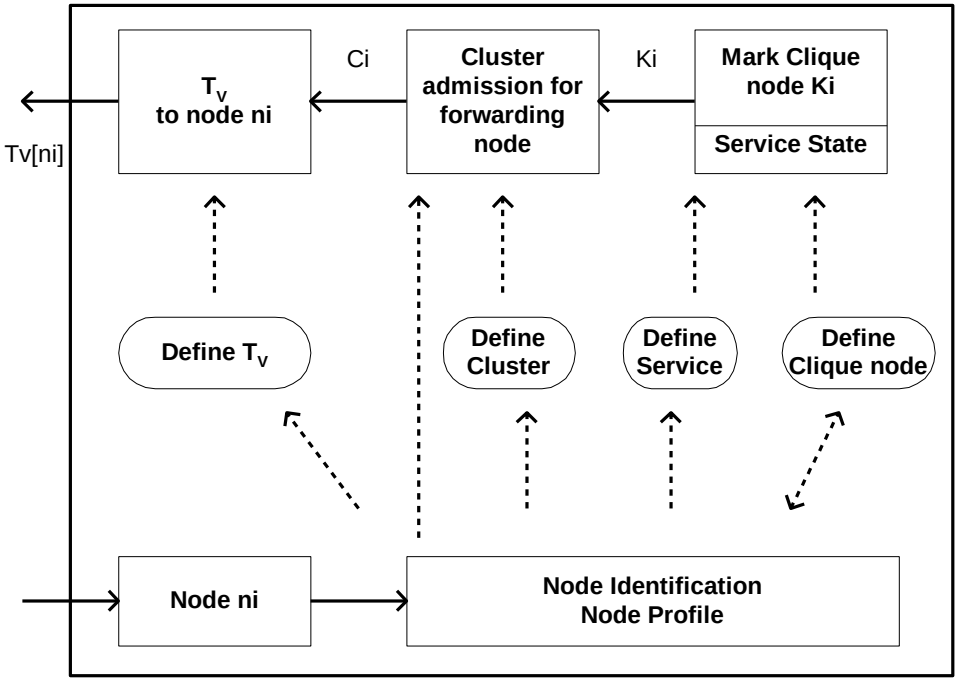

Fig 3: Trust Value (Tv) for node

The Tv assigned to node ni is alive until it satisfies any one of the following conditions, where (a) a node leaves or a new node joins the cluster (b) time to be alive value for the node expires (c) when the cluster gets updated or (d) when the session is completed.

Algorithm 1*: SKEMA Algorithm (Pseudo code format)*

For i = 1 to n do

Begin

1 : Initialize ( ) // initialize all nodes in N and in Cluster C

2: Select_SKEMACoordinator (node[i], KTv) // poll election algorithm to select coordinator node

3: REQ_SKEMA (Ci, n[i]) // request Trust Key for node 'i'

4: ST := GatherProfile(i, ToS,) // profile of node and type of service

5: SKEMA_Trustkey(KTv_value) // generate trust key

6: n [i] = Assign (Tkv_value, Ci) // Ci being the cluster head node

7: RPY_SKEMA (Ci, n[j]) // key exchanged with neighbour node

EndFor

Generation of Trust Value is discussed in Algorithm 2. The Trust Value (Tv) generated for node 'ni' can be assigned if and only if the node 'ni' satisfies section 3.1.2 [A].

Algorithm 2 *: SKEMA – Trust Value Assignment*

1: Initialize Trust value Tv- for nodes, n = 1, . . . ,N and Cluster C = i,j,k…..m

2: Mark Clique node size Kn_i *= 1,2,..k*

3: $\forall$ *node targets ni do step 4 to 7*

4: Find overlapping and non overlapping cluster of nodes 'n' AND ($ni \subset Ki$ *) OR (* $ni \in Ci$ *)*

5: $Tv[ni] \rightarrow log(ni)^n . \sum_{i=1}^{k} \binom{n}{k} rand((Ki) * ni^{(n-k)})$ *//*

defining trust value

6: for $\forall$ *node* $ni \subset Ki$*, where i = 1,2…k do*

7. Update Tv for node 'ni'

8: $\forall$ *nodes ni,nj where* $n \subset Ci$ *and* $n \in Ki$

Assign (Tv[ni], tta)

Assign (Tv[nj],tta)

9: Update_Trust (ni, Tv, tta)

10: If node $ni \not\subset Ci$ *AND* $ni \notin Ki$*, then Remove node 'ni'*

11: Loop Step 6:

12: Return

5. EXPERIMENTAL APPROACH

ns2 simulation tool [12] was used to compare the performance between CLIQUES, PROFIDES and SKEMA security scheme. Table 1 shows the test bed parameters used to compare the protocols using ns2. A total of 3 test beds were configured to support in security analysis of schemes such as CLIQUE, PROFIDES and SKEMA scheme. Different test beds were created by varying the number of nodes, service and packet size (based on the application).

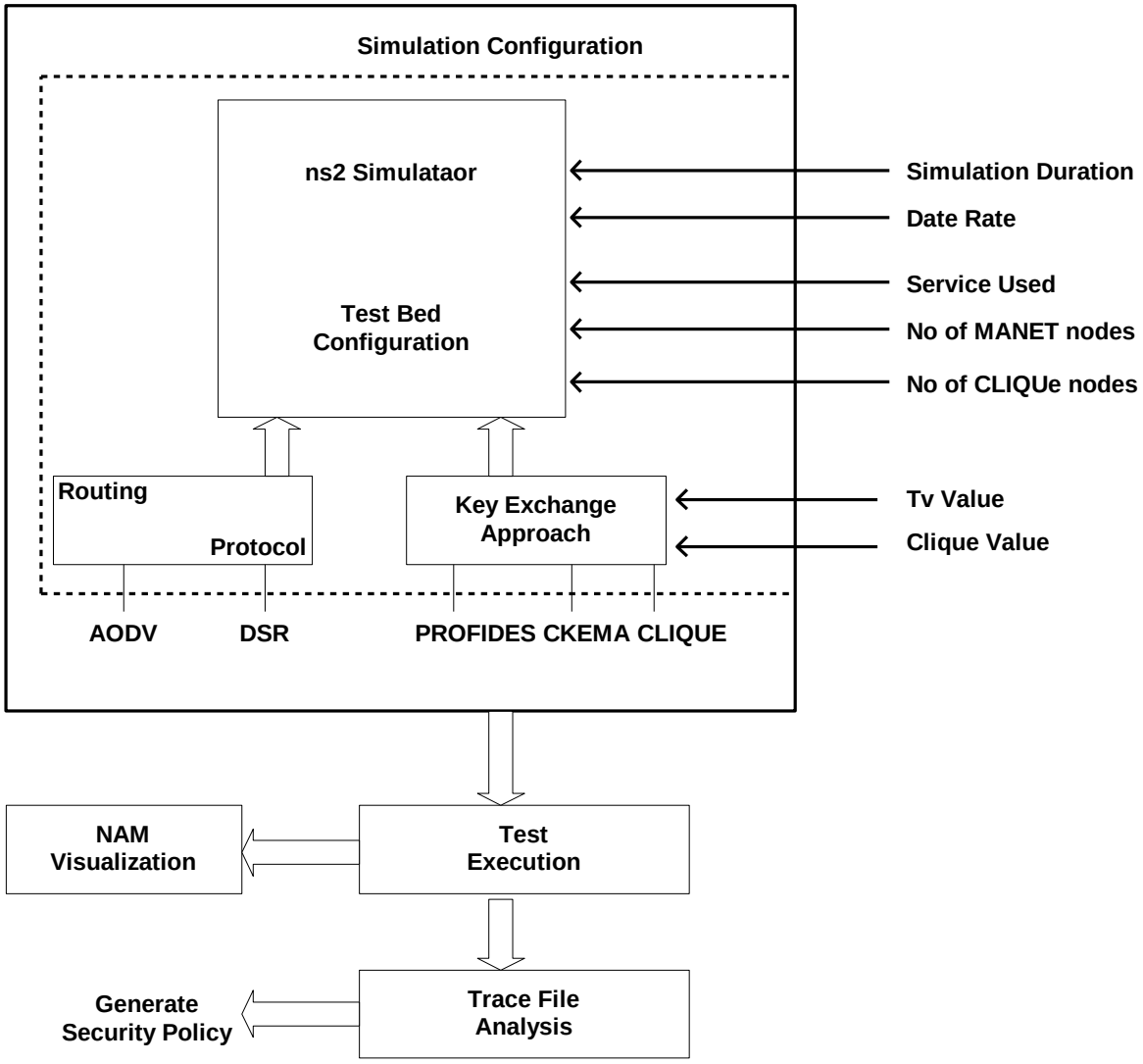

Fig 4: Test bed Analysis and configuration

The test bed configuration module [Fig. 4] configures the parameters required for the test. The Key Exchange Approach module configures the secured key exchange scheme and its parameters for an application to provide a service over a network. The routing protocol configuration module specifies the protocol that simulator should use as the routing protocol such as AODV. As AODV is well taken by research community to implement over MANET networks, the proposed SKEMA scheme for security is implemented. The experiment was carried out by introducing unsecured nodes and embedding anomaly based nodes during configuration.

Table 1. ns2 Simulation Parameters

Parameter	**Value**
Simulation Duration	100s
Simulation Area	500 x 500
No of nodes	35
Transmission Range	250mts
Node Movement	Random Way Point
Packet Type	CBR (UDP)
Data Payload	512 bytes
Maximum speed	1 – 25 m/s
Routing protocol used	AODV
Anomaly nodes introduced	10

The random traffic connection of CBR is set up between mobile nodes using traffic–scenario generator script. In order to create a traffic connection file, the type of traffic connection, the maximum number of connections to set up between them and a random seed can be generated. In ns-2 test simulations being conducted, 35 MANET nodes are placed randomly within a 500 m by 500 m area, where twenty different random scenarios are simulated. The packet size adopted in simulations is 500 bytes while the bandwidth is 2 Mbps. Multiple source and destination pairs were randomly selected to simultaneously transmit services as video, on demand data and text data as randomly chosen data flow join in for each 10ms. The total simulation time is 100 seconds for each experiment. UDP is used as the underlying transport layer protocol for both the real-time and the non-real-time streams.

5.1 Performance Analysis

Performance of SKEMA scheme was tested over AODV routing protocol over 35 nodes at 100 seconds. Various test scenarios were adopted, since the performance of SKEMA can be understood based on maximum number of sessions being maintained, when anomalies are introduced.

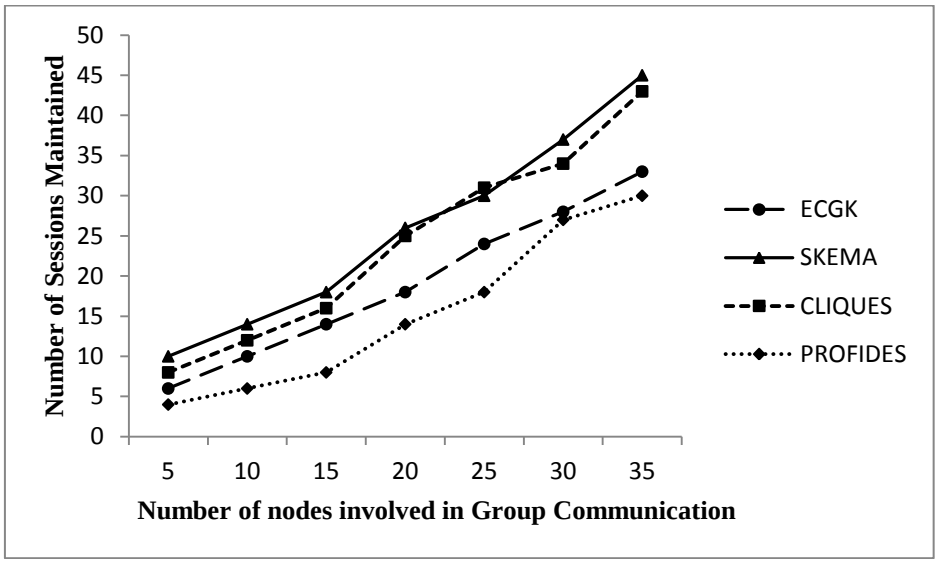

Fig 5: SKEMA for Session Maintenance

Fig. 5 shows the behavior of SKEMA for an average maximum number of sessions maintained for multiple nodes involved in group communication. It could be seen that both SKEMA and CLIQUE schemes manage an average of 45% of sessions for an average of 20 to 25 nodes, while SKEMA is found to handle an average of 50% of sessions when number of nodes increments. To understand the security and fault tolerant behavior of SKEMA based on increase in traffic intensity (Fig. 6).

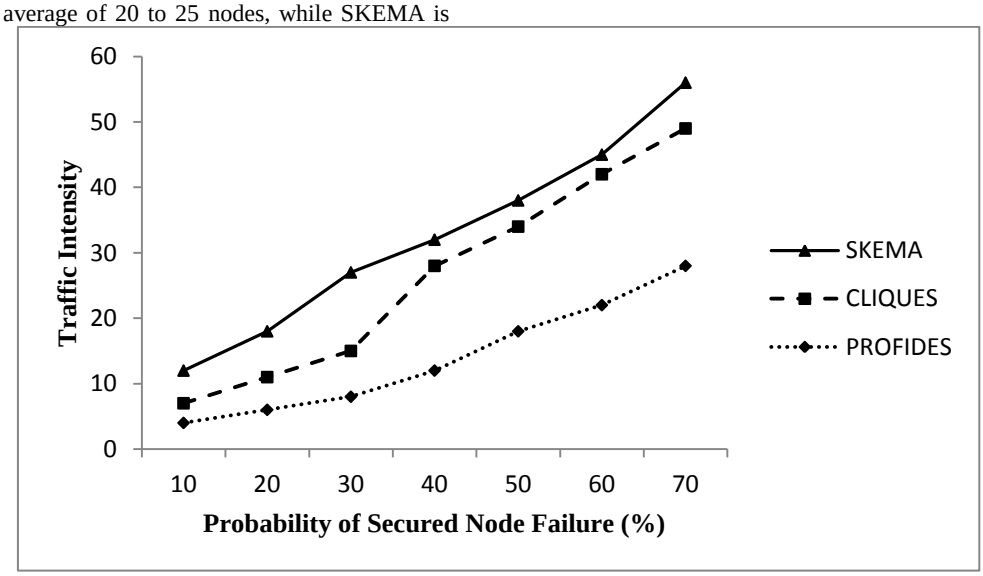

Fig 6: Secured node failure based on traffic intensity

SKEMA exhibits reduced chances of secured node failure due to anomaly attacks, while PROFIDES confirms similar chances of node failure as similar to CLIQUES scheme. Key exchange method among active nodes involved in communication is the primary factor which manages fault tolerance.

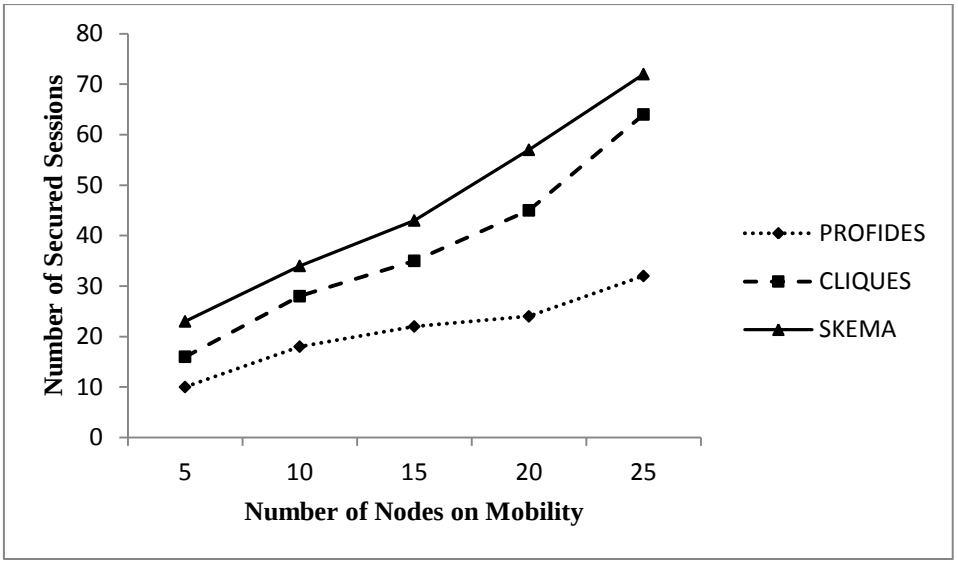

Fig 7: Secured sessions

Handling the secured sessions is explained in Fig. 7, SKEMA confirms an improved number of secured sessions, compared to CLIQUE and PROFIDES. It could be found from Fig. 7 that as number of MANET nodes increases, the percentage of secured sessions increases for SKEMA and PROFIDES sequentially. Performance analysis of SKEMA verified using various test carried out confirms adaptive security compared to CLIQUE and PROFIDES scheme, which are well represented in survey.

6. CONCLUSION

A mobile ad hoc network (MANET) is a wireless network without centralized administration or fixed network infrastructure. Self-organization, decentralization and openness are advantages, but these characteristics also introduce insecurity. Traditional routing protocol of MANET such as AODV, DSR, TORA does not consider the adaptive security mechanisms for data or session management over variable services.SKEMA focuses on an adaptive security mechanism to support AODV over MANET. The nodes are grouped or clustered based on clique graph, which acts as coordinator to distribute the keys among multiple clusters. The key exchange is carried out only among active nodes, hence minimizes processing and redundancy of storing the secured key among in active nodes. SKEMA is experimented using ns2 simulator and found that its performance is improved than compared to CLIQUE and PROFIDES schemes. The future work can be extended towards dynamic recommendation system to support in security among dynamic nodes.

7. REFERENCES

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, fifth edition, 1996.

[2] Arunkumar Thangavelu, Senthilkumar S, Chapter-21:Knowledge on Routing Nodes in MANET: A Softcomputing Approach, Case Studies in Intelligent Computing : Achievements and Trends, CRC Press, Taylor and Francis Group, pg-427 -450, 2014

[3] Balasubramanian A., Misha, S., Sridhar, R., "A Hybrid approach to key management for enhanced security in ad hoc networks", Technical report, university at Buffalo, NY, USA,2004

[4] Bing Wu, Jie Wu and YuhongDong,"An efficient group key management scheme for mobile ad hoc network", International Journal and Networks, Vol. 2008

[5] Bernard Barber. Logic and limits of Trust. New Jersey: Rutgers University Press, 1983

[6] Boyd C, Mao W, Paterson KG. Key agreement using statically keyed authenticators. In: Proceedings of the second international conference on applied cryptography and network security, 2004. p. 248-62.

[7] George Theodorakopoulos and John S. Baras, On trust models and trust evaluation metrics for ad hoc networks. IEEE Journal on Selected Areas in Communications, 24(2):318–328, February 2006

[8] K. Hoeper and G. Gong. Key Revocation for Identity-Based Schemes in Mobile Ad Hoc Networks, International Conference on AD-HOC Networks & Wireless (AD HOC NOW `06), LNCS 4104, Springer Verlag, pp. 224-237, 2006.

[9] K. Hoeper and G. Gong. Pre-Authentication and Authentication Models in Ad Hoc Networks, book chapter in Wireless Network Security, edited by Y.Xiao, X. (Sherman) Shen, and D.-Z. Du, Springer Verlag, ISBN: 978-0-387-28040-0, 2007.

[10] Imad Aad , Jean-Pierre Hubaux , Edward W. Knightly, Impact of denial of service attacks on ad hoc networks, IEEE/ACM Transactions on Networking (TON), v.16 n.4, p.791-802, August 2008

[11] National Institute of Standards and Technology (NIST), Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2006

[12] Network Simulator NS-2. http://www.isi.edu/nsnam/ns/.

[13] R.C.W. Phan. Fixing the Integrated Diffie-Hellman-DSA Key Exchange Protocol, IEEE Commun. Letters, vol. 9, no. 6, pp. 570-572, 2005.

[14] K.G. Paterson. Cryptography from Pairings: a Snapshot of Current Research, Information Security Technical Report, vol. 7, no. 3, pp. 41-54, 2002

[15] Qing Chen, Zubair Md. Fadlullah, Xiaodong Lin, Nei Kato, A clique-based secure admission control scheme for mobile ad hoc networks (MANETs), Journal of Network and Computer Applications, Vol34 Issue 6, November, 2011, pg 1827-1835

[16] Rachedi A, Benslimane A, Guang L, Assi C. A confident community to secure mobile ad-hoc networks. In: ICC 2007. Glasgow, Scotland, UK, 2007.

[17] Renu Dalal, Yudhvir Singh and Manju Khari, A Review on Key Management Schemes in MANET, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012, pg 165-173

[18] R. Saminathan, Dr. K. Selvakumar, "PROFIDES - Profile based Intrusion Detection Approach Using Traffic Behavior over Mobile Ad Hoc Network", International Journal of Computer Applications 0975 – 8887 Volume 7– No. 14, October 2010.

[19] R. Saminathan, K. Selvakumar, TRUCE – An Adaptive Trust Management Algorithm Over MANET for Service-Based Mobile Computing Environments, Information Security Journal: A Global Perspective , Volume 20 Issue 4-5, Pages 173-184, January 2011

[20] Senthilkumar K, Arunkumar Thangavelu, Classification and prediction of routing nodes behavior in MANET using fuzzy proximity relation and ordering with Bayesian classifier', IEEE Int. Conf. on Pattern Recognition, Informatics and Mobile Engineering, PRIME-2013, Feb 21-22, 2013, pp.454–460

[21] Senthilkumar K, Arunkumar Thangavelu, Trust Evaluation using Fuzzy proximity relation with ordering for MANET', Int. J. Trust Management in Computing and Commu.,Vol. 1, No. 2, pp.105–120, 2013

[22] Wu, B., Wu, J., Fernandez, E., Ilyas, M. and Magliveras, S., "Secure and Efficient key Management in mobile ad hoc networks", Network and Computer Applications, Vol. 30, pp. 937-954, 2007.

[23] Weimerskirch and D. Westho, Identity Certified Authentication for Ad-hoc Networks, Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN), 2003, ACM Press, ISBN: 1-58113-783-4, pp. 33-40, 2003

[24] S. Vasudevan, J.Kurose, D. Towsley, " Design and Analysis of a leader election algorithm for Mobile AdHoc Networks", Proc. IEEE International Network Protocols, 2004, pg 122-130

[25] Yun Teng, Vir V. Phoha, and Ben Choi. Design of trust metrics based on dempster-shafer theory. http://citeseer.nj.nec.com/461538.html

[26] Vikram Srinivasan, Pavan Nuggehalli, CarlaFabiana Chiasserini, and Ramesh R. Rao. Cooperation in wireless ad hoc networks. In INFOCOM' 03: Proceedings of IEEE Conference on Computer Communications, 2003.

[27] Y. Zhang, W. Liu, W. Lou, and Y. Fang. Securing Mobile Ad Hoc Networks with Certificateless Public Keys.IEEE Trans. Dependable Secur. Comput. , vol. 3, no. 4, pp. 386-399, 2006.