Scalable and Secure Dynamic Key Management and Channel Aware Routing in Mobile Adhoc Networks

K. Selvakumar[1], N. Seethalakshmi*[2]
[1]Department of Information Technology, Faculty of Engineering and Technology, Annamalai University, India
[2]Department of Computer Science and Engineering, Faculty of Engineering and Technology, Annamalai University, India

Article Info

Article history:

Received Nov 9, 2017
Revised Jan 17, 2018
Accepted Feb 12, 2018

Keyword:

Black hole attack
Cluster head election
Destination-sequenced distance vector
Mobile adhoc networks
RSA

ABSTRACT

A MANET (Mobile Ad-hoc Network) is an infrastructure-less self configuring wireless networks of routers. Key management is at the center of providing network security via cryptographic mechanisms with a high-availability feature. Dynamic key is the efficient assistance for network scalability. Routing protocol used here is a form of reactive routing called CA-AOMDV and compared with Table driven routing called DSDV. Channel aware routing protocol quality of the channel which can be measured in terms of suitable metrics. This paper leads to an emphasis on Black hole attack and to develop a dynamic key framework using RSA algorithm.

Corresponding Author:

N. Seethalakshmi,
Department of Computer Science and Engineering,
Faculty of Engineering and Technology, Annamalai University,
Chidambaram, Tamilnadu, India – 608 002.
Email: seethan1989@gmail.com

1. INTRODUCTION

Security is one of the major issues in MANETs. Their natural characteristics make them vulnerable to passive and active attacks, in which misbehaving nodes can eavesdrop or delete packets, modify packet contents, or impersonate other nodes [1].

A keying processis the state in which network nodes share keying information for use in cryptographic mechanisms. Peer Intermediaries for Key Establishment (PIKE):-PIKE deploys the sensor nodes to initiate the shared key. PIKE is symmetric key agreement system, it using unique secret key in a group of nodes .This method is using the concept of random key pre-distribution, and in 2-D case with each of the O (n) nodes each mobile node contributes a unique secret key in horizontal and vertical dimension [2]. In SEGK, to create a familiar group key, each group memberachieves a share of the final common group key. The group key can be refreshed periodically or only be refreshed in response to changes of group membership. The updating of the group key improves to enforce backward and forward secrecy of group communications [3].

Self Organized Key Scheme (SOKS):In the self organized network each mobile node represents as a different CA.SOKS was disclosed. It has very low scalability and low resource efficiency but possess the off line authentication and restricted intrusion detection security services. SOKS having high intermediates encoding operations and high storage cost [2].

Zone-Based Key Management Scheme:- ZRP (Zone Routing Protocol), in this model for each mobile node zone is described. Some existing number is assigned to each mobile node which relays on the distance in hops. Symmetric key management is treated by mobile node only for intra or inside r zone (zone radius). Clustering mobile node uses asymmetric key management for inter-zone security without depends on it. It allows effective way to making the public key without destroying the capability of making the certificates [2].

We give an efficient solution to distribute in a dynamic way the role of the PKG by conveniently using a bi-variate polynomial to share the master key. Subsequently, this construction gives a solution to mutually perform the role of the PKG in a mobile ad-hoc network [4]. DKPS model to acknowledge completely distributed and self organized key pre-distribution without relying on any infrastructure support. This technique of implementing DKPS avoided the limitations of the traditional techniques.

DKPS needs less storage as contrasted to pair-wise key accord way [5]. DKPS symmetric key management scheme is much effective when compared to group key schemes and pair wise key agreement. DKPS is highly secure and effective methods when compared to any other symmetric key management method [6]. Since homomorphism and non-trivial zero encryption properties of DKPS, either side can only discover the common secret key, without disclosing the other non-common keys [7].

AODV is a dynamic routing protocol that creates and maintains the routes only when they are needed. [8] AODV is composed of two essential functions namely route discovery procedure and route maintenance procedure. Ad Hoc on Demand Distance Vector Routing (AODV) is additionally on-demand routing protocol. It utilizes customary routing tables, one section for every destination [9-11]. In AODV [12], just a single route path is accessible in routing table, if this path falls flat, it again starts route discovery process to discover another optimum path. Route Request Message (RREQ) from the source to the destination and route reply message (RREP) from the destination to the source. To conquer this limitation, Ad Hoc Multipath Distance Vector (AOMDV) comes into account.

One of the conflicting issues in DSDV is that it doesn't maintain load of traffic in large scale MANET and delay. Hence, it can be said that neither AODV nor DSDV [13] should be considered as most efficient energy effective routing protocol till date, as it even doesn't address the basic QoS issues in MANET. Hence, there is a need of formulating a new routing protocol with completely new considerations and technical assumption that can ensure energy effectiveness in MANET. The term "channel-aware" in our work refers to having the knowledge of channel conditions. The term condition mentions to the quality of the channel which can be measured in terms of appropriate metrics [14].

Channel Aware AOMDV (CA-AOMDV) uses the channel average non-fading duration as a routing metric to choose fixed links for route discovery, and applies a preemptive handoff strategy to keep reliable routes by exploiting channel state information. Using the identical information, routes can be used again as they become available again, rather than being desirable. We provide new theoretical results for the downtime and lifetime of a live-die-live multiple path system, as well as detailed theoretical expressions for common network performance measures, providing useful insights into the differences in performance between CA-AOMDV and AOMDV [9].

Internal threats due to changes in the node behavior that target the routing discovery or maintenance phase of the routing protocol (CA-AOMDV) which applies a preemptive handoff strategy to maintain reliable connections by exploiting channel state information [10]. By utilizing the Advance Multi route AODV and Channel Aware routing protocol we can not only decrease the network congestion by reducing flooding, occurred due to rapidly finding the destination in continuously changing topology, but also, it provide the guarantee of completion of data transmission in the case of link failure [11].

Channel aware routing protocol will be used in heterogeneous system [15].In MANETs routing, the node failure occurs due to two reasons. One is link failure and other is node overloaded. In this LBCA-AOMDV, we have concentrated on node over loaded by the threshold value. Here we fix the threshold values, if any node exist that particular value consider that node will be overloaded and it comes away from the path and not from the channel. The particular load is replaced by some neighboring node [16].

A secure key management system for group based a MANET that does not rely on a centralized authority for creating and distributing keys. Group heads create, generate, and distribute the keys in their groups in a secure manner [17]. The benefit of this security method is that since encryption is done twice with two different encryption methods, one with neighborhood key and another with message specific key, more security is imposed. Whenever the topology changes with the inclusion or exclusion of a member, new neighborhood key is computed and is distributed to all authenticated neighbors. Message storage at the node level and compare the performance of spanning tree with and without the inclusion of features such as key storage and message storage are not done here [18].

A Ternary tree based Group ECDH.2 (TGECDH.2) protocol that deploys a group of rekeying method during membership change. This tree is a balanced key tree in which suitable insertion point is chosen for joining the members during rekeying process. This protocol merges the computational effectiveness of ECDH protocol and the communication efficiency of GDH.2 protocol [19].

We have planned and possessed a Dynamic Key Length Based Secure Frame-work (DLSeF) to supply end-to-end security for big data stream processing. This approach [20] is based on a common shared key that is produced by exploiting synchronize prime number. The proposed scheme avoids excessive communication between data sources and Data Stream Manager (DSM) for the rekeyingmethod. Hence, this leads to reduction in the overall communication overhead. Because of the reduced communication overhead, our approach is able to perform security verification on-the-fly (with minimum delay) with least computational overhead.

Shared key encryption is very simple and fast which would arrange MANET data exchange faster. If the key is believed to be compromised, a new key can be found. No intermediate node can predict the key unless most of the intermediate nodes are compromised. Main drawback of this protocol is: if the number of routes are small and one or more nodes are common to all the routes then that particular node(s) can compute the key. But the receiving node can decide such circumstance and discard such key and produce a new one. Moreover if the nodes have mobility, they can change their geographical location to discover the key stronger [21].

While static schemes basically assume that administrative keys will outlast the system and underline pair-wise communication keys, dynamic schemes advocate rekeying to accomplish flexible to attack in long-lived networks and primarily emphasize group communication keys. Dynamic key management schemes may change administrative keys occasionally, on request or on detection of node capture. The most important advantage of dynamic keying is refreshed network survivability, because of any captured key(s) is exchanged in a timely manner in a process known as rekeying. Another benefit of dynamic keying is providing better support for network expansion; upon adding new nodes, unlike static keying, which uses a fixed pool of keys, the probability of network capture does not necessarily increase. Both homogeneous and heterogeneous dynamic key management schemes have been proposed in the literature [22].

The random pair-wise scheme has the most suitable security properties of the three schemes that belongs to perfect resilience against node capture attacks as well as support for node based revocation and resistance to node replication. The properties join with the trade-off that the high supported network size is not as high as the other schemes [23].

A new encryption technique called Variable size Block Encryption using Dynamic-key Mechanism (VBEDM), which is designed with unlimited key size, dynamically changing permutation table based on the encryption key and variable block size for each round. To make the cryptanalyst difficult to make the plain text from the variety of compression algorithms the VBEDM used a compression technique based on key [24].

It is difficult to detect patterns with which to perform cryptanalysis on the dynamic key. Here the authors have presented concept of dynamic key with symmetric cryptography. Dynamic key is like to one time pad. A dynamic key theory is described and mathematically analyzed. Here author produced a cryptography system in which four rounds of encryption & decryption are performed. In each round, various parts of dynamic key are connected to make it hard against cryptanalysis attacks [25]. A Secure & Efficient Audit Service Outsourcing method designed to prevent the fraudulence of prover [26]. An efficient mechanism on probabilistic queries and periodic verification is proposed to reduce the audit costs per verification and implement abnormal detection timely [27].The link level congestion occurs when more than one sensor node tries to acquire the channel at same time. In case of link-level congestion, all the nodes attempt to send traffic on the link simultaneously. It results in packet collisions. Furthermore, due to link-level congestion, the link utilization is reduced. To avoid all the above-mentioned effects of congestion, congestion must be controlled or avoided in an effective way [29]. Heterogenous network have budding to improve network lifetime and also provide sophisticated quality network. Due to limited power battery will exhausted. Thus, energy efficient routing protocol needs to allocate the balance energy burden between the sensor nodes [28]. In this study, a scalable dynamic keying technique called DKT for Mobile Adhoc network has been proposed.

2. DYNAMIC KEY MANAGEMENT FOR MANETs

In this study, a scalable dynamic keying technique called DKT for Mobile Adhoc network has been proposed. At first the nodes are assembled into different clusters as per the distance. The GPS enabled nodes are chosen as CHs. With the assistance of CH, all the cluster members can assess their locations. Each cluster member additionally evaluates its node degree by calculating its neighbors. The CH has a member table which contains the details of every member id, its area, node degree and virtual battery power to deliver one packet to the CH. The key utilized for the encryption dynamically replaces according to the capacity of the

CCV. So the procedure of re-keying is not needed. In this way, separate dynamic keys are produced in each cluster by the CH. Proposed system expresses the workflow representation in steps by-steps in Figure 1.

2.1. Cluster Formation

The process of group of nodes includes a subgroup and nominates a head known as cluster head (CH). To choose efficient CH, first weight will be calculated for each and every node in the network. To start with weight calculation process every node is identified by unique ID and all other nodes compute their individual weight based on difference of Degree, Energy (battery power), Distance and speed of the model. The Equation (1) is used for calculating weight value for mobile node.

$$\mathrm{N_n = N_1^*\Delta_n + N_2^*E_n + N_3^*M_n + N_4^*D_n} \tag{1}$$

where $\mathrm{W_n}$- weight of node 'e'

Δ_n - Degree Difference of node 'e'

$\mathrm{E_n}$– node's energy 'n

$\mathrm{M_n}$–node's mobility 'e'

$\mathrm{D_n}$ - Distance from node 'e'

N1, N2, N3, N4 - co-efficient

The co-efficient are assigned with the values, N1 = 0.5, N2 = 0.35, N3 = 0.05, N4 = 0.1 and the total of these coefficient is 1. The difference of Degree and Battery Power are taken fundamentally and allocated with higher values 0.5 and 0.35. The weight values are kept in every node with its unique ID and these are send out to neighbors to elect CH.

2.2. Cluster Head (CH) Nomination

The proposed algorithm constitutes Cluster Head nomination and Cluster Head lifetime observing algorithms respectively. The Secondary Cluster Head (SCH) additionally chose to maintain distance from bottlenecks while the death of CH.

Cluster Head Election Algorithm

```
Step 1: Compute weight for each node based on the parameters like Node Degree, Mobility, Connectivity and Energy Remaining.
Step 2: Broadcast Weight value and its unique Id to all its Neighboring nodes and the neighborhood table refreshed with weight value.
    Step 3: CH and SCH chose based on the weight value.
    If (The Node with most elevated weight value).
    Choose that Node as a CH.
    If (The Node with next most elevated weight).
    Choose that Node as a SCH.
    Else, Normal nodes send Join request to CH to create a Cluster.
```

Cluster Head Lifetime Algorithm

```
SCH observe the battery level of CH for each 25s.
If (Battery level of CH < Minimum Threshold Level).
SCH will turn out to New CH,
Send CH_LIFE DOWN Message to all member nodes,
Election method started to discover new SCH.
Else,
Re election not required.
```

2.3. Dynamic Key Distribution

After the nomination of Cluster Head, it starts the dynamic key generation process using dkps scheme in channel aware routing protocol by gathering cluster members ID and public key. Below algorithm represents procedure of computing DK in channel aware routing protocol.

The Equation 2, that represents dynamic key calculation using RSA algorithm.

$$\mathrm{DK}=(\left(\propto^{\mathrm{k_1+k_2+k_n+CHD_k}} \mathrm{modpn}\right)\mathrm{X}\,(\mathrm{RD_V}) \tag{2}$$

where GK is the group cluster

$\propto$is the primitive root of p
$\mathrm{CHD_k}$ is the private key of cluster head
$\mathrm{k_1,k_2,\dots k_n}$ private members Public keys
pn is the prime number
$\mathrm{RD_V}$random value generated while renewing the DK secretly.

The distribution of dynamic key is started with the encryption of DK by Cluster head and decodings in the next end completely the cluster members using RSA algorithm in channel aware routing protocol. Below represents the algorithm for encryption and decryption in key distribution.

Dk Generation Algorithm

```
Step 1:
If (Node exist inside the cluster)
If CH obtains public keys of all nodes
compute dynamic key as follows:

CH: DK=($(\propto^{\mathrm{k1+k2+\cdots.Kn\ +CHDK}}\ modpn)X\ (RD_V)$
End if
End if
```

Encryption and Decryption for Key Distribution Algorithm

```
Step 1: CH → nodes inside the cluster:
        Encode DK using RSA algorithm
        E (DK) = ((DK) en mod np) in which {en, np} are public key pair.
Step 2: Decode DK in Nodes:
        D (DK) = (E (DK)dn mod np) in which {dn,np} are private key pair.
```

2.4. Authentication

In channel aware routing protocol inside the cluster, if any two nodes hope to communicate first it will authenticate each other. For example node aand b becomes authenticated nodes by using following algorithm.

Algorithm - Providing Authentication between Node X and Y

```
Step 1: Node a → b: hash value using (Node (a) id, public key, DK) and its unique id, public key.
Step 2: Node a: compute new value (Node (a) id, public key, DK).
Step 3: If received and computed values are same then Node a becomes authenticated.
```

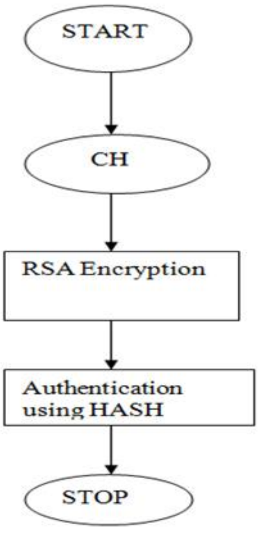

Figure 1. Flow chart for our proposed method

3. RESULTS AND DISCUSSIONS

A malicious node, the so called black hole node, may always respond positively to route requests even when it does not have proper routing information. The black hole can drop all packets forwarded to it . The figure below shows the Black Holes detected in a 10 to 100 nodes keeping speed constant to 2 m/s. The metrics chosen are Packet Delivery ratio, delay, throughput, packet overhead and energy.

According Figure 2-6, The proposed method detected black hole attack for 1 & 5 attacker with 100 nodes behalf of PDR (Packet Delivery Ration) Delay, Throughput, packet overhead and energy consumptions. Based on observation of graphical result Figure 2-6, Its claims that proposed methods performs well compare than other existing methods.

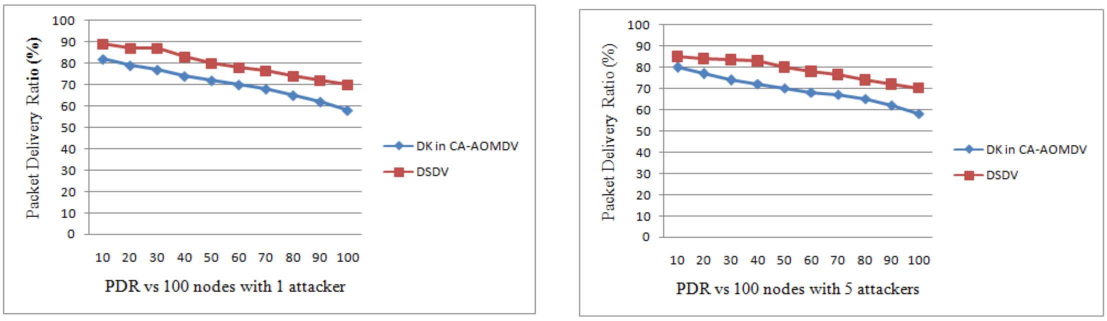

Figure 2. Black hole attack detected in proposed method in terms of PDR using 1 and 5 attackers respectively

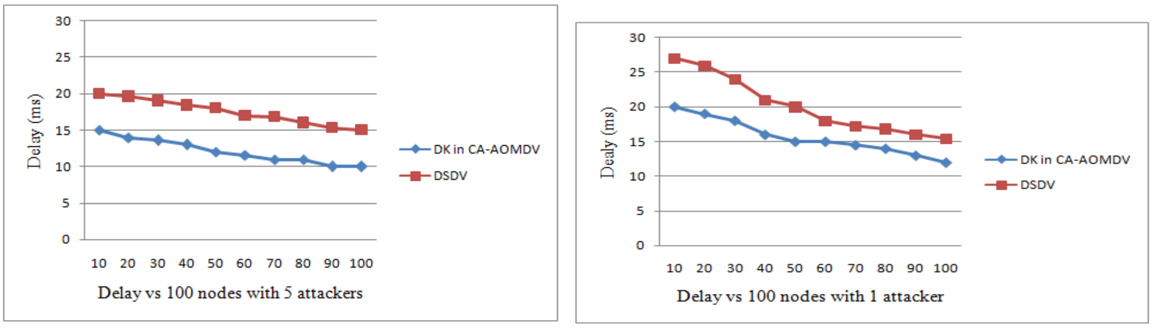

Figure 3. Black hole attack detected in proposed method in terms of delay using 1 and 5 attackers respectively

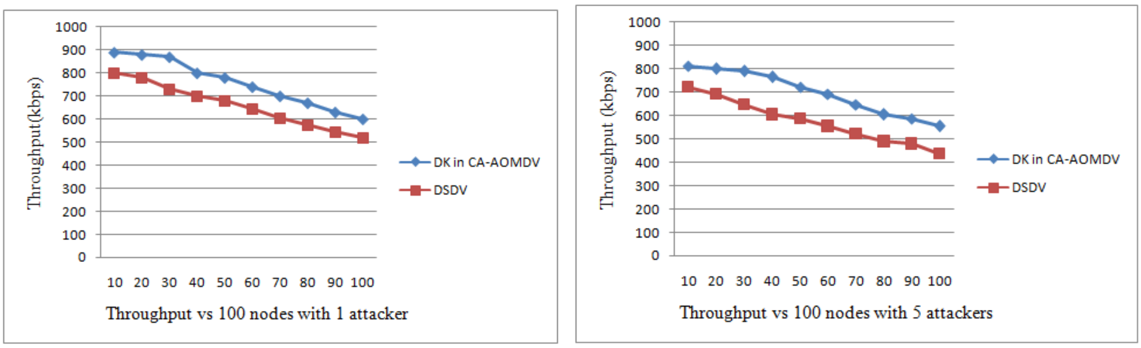

Figure 4. Black hole attack detected in proposed method in terms of throughput using 1 and 5 attackers respectively

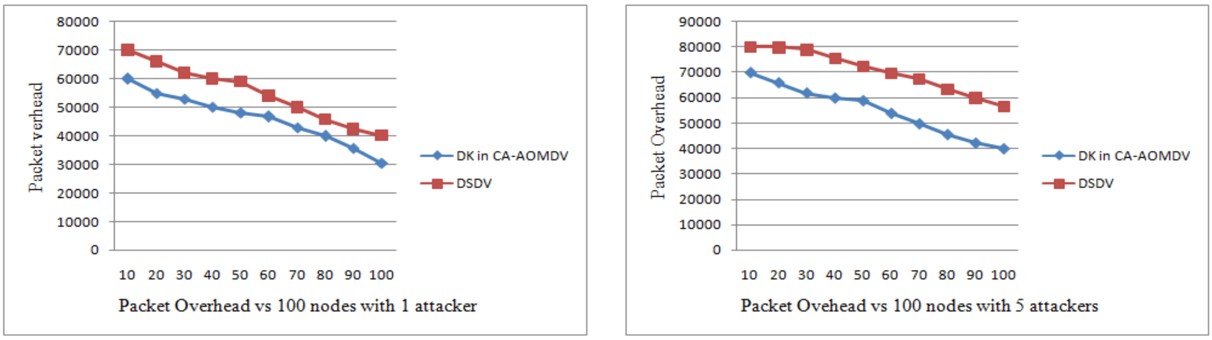

Figure 5. Black hole attack detected in proposed method in terms of packet overhead using 1 and 5 attackers respectively

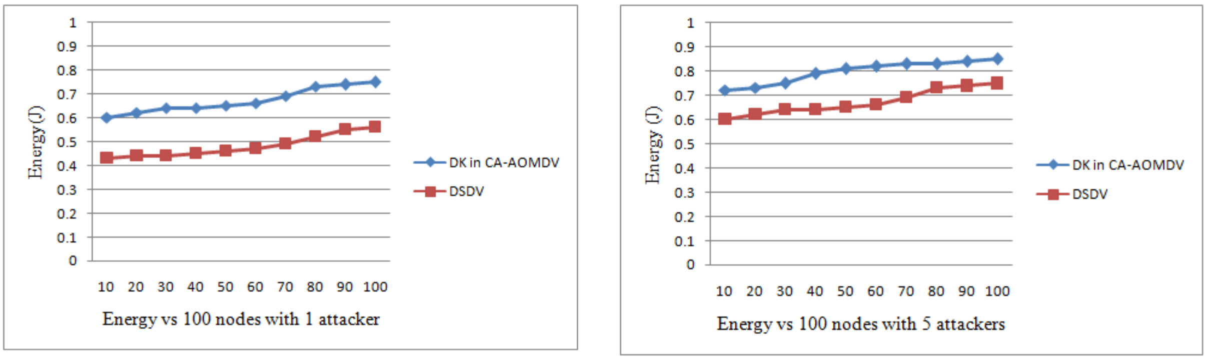

Figure 6. Black hole attack detected in proposed method in terms of energy using 1 and 5 attackers respectively.

4. CONCLUSION

In this, the issues related to security and the loopholes of CA-AOMDV and DSDV protocols, has been studied specific to the network layer attacks such as black hole attack and wormhole attack. A dynamic key generation and distribution is implemented using RSA algorithm and tested with networks of varied node configurations that gives higher computational complexity. It performs better in terms of packet delivery ratio. Security comes with decrease of packet drooping and minimizing delay. CA-AOMDV is not affected by black hole due to some of the attacks are secured by dynamic key proposed.

REFERENCES

[1] Eduardo da silva, Aldri l. Dos santos, and luiz carlos p. Albini, “Identity-Based Key Management In Mobile Ad Hoc Networks: Techniques And Applications”, *IEEE Wireless Communications*, vol.15, no. 5, pp. 46-52, 2008.

[2] Renu Dalal1,Yudhvir Singh and Manju Khari, “A Review on Key Management Schemes in MANET”, *International Journal of Distributed and Parallel Systems*, vol. 3, no. 4, pp. 165-172, 2012.

[3] Bing Wu, Jie Wu and Yuhong Dong., “An efficient group key management scheme for mobile ad hoc networks”, *Int. J. Security and Networks, Inderscience Enterprises Ltd.*, vol. 4, no. 1-2, pp. 217-226, 2008.

[4] Vanesa Daza, Paz Morillo and Carla Rafols., “On Dynamic Distribution of Private Keys over MANETs”, *Electronic Notes in Theoretical Computer Science*, vol. 171, no. 1, pp. 33-41, 2007.

[5] Nisha Sharma, Dr.Sugandha Singh., “Approaches in Key Management Schemes in Mobile Ad-Hoc Networks: A Review”, *IOSR Journal of Computer Engineering*, vol. 18, no. 4, pp. 10-14, 2016.

[6] K.E Hemapriya, K. Gomathy., “A Survey Paper of Cluster based Key Management Techniques for Secured Data Transmission in Manet”, *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 10, pp. 511-518, 2016.

[7] C.Shanmuganathan, Dr.P.Raviraj., “Different Approaches for Secure and Efficient Key Management in Mobile Ad-Hoc Networks”, *International Journal of Modern Trends in Engineering and Research*, vol. 2, no. 1, pp. 552-560, 2014.

[8] S. Ashok Kumar, E. Suresh Babu, C. Nagaraju, A. Peda Gopi., "An Empirical Critique of On-Demand Routing Protocols against Rushing Attack in MANET", *International Journal of Electrical and Computer Engineering (IJECE),* vol.5, no. 5, pp. 1102-1110, 2015.

[9] Xiaoqin Chen, Haley M. Jones, and Dhammika Jayalath., "Channel Aware Routing in MANETs with Route Handoff", *IEEE Transactions On Mobile Computing*, vol,10, no. 1, pp. 108-121, 2011.

[10] Dr. V.kavitha and S.Balaji., "ESAC Based Channel Aware Routing Using Route Handoff", *International Journal on Computer Science and Engineering,* vol. 3, no. 3, pp. 1260-1269, 2011.

[11] Shubham Baronia., "Advance Channel Aware AODV Routing Protocol in Mobile Ad hoc Network", *International Journal of Engineering Technology & Management Research,* vol. 1, no. 1, pp. 61-66, 2013.

[12] Rahul Desai, B P Patil, Davinder Pal Sharma., "Routing Protocols for Mobile Adhoc Network: A Survey and Analysis", *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. 7, no. 3, pp. 795-801, 2017.

[13] Ramanna Havinal, Girish V. Attimarad, M. N. Giri Prasad, "EASR: Graph-based Framework for Energy Efficient Smart Routing in MANET using Availability Zones", *International Journal of Electrical and Computer Engineering (IJECE),* vol. 5, no. 6, pp. 1481-1395, 2015.

[14] Sridhar K N and Sridhar K N*., "Channel-aware Packet Scheduling for MANETs",* In World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008. 2008 International Symposium, pp. 1-9, 2008.

[15] Mr.B.V.Baiju and Mr.Sudhakar Rajendran., "Channel Aware Routing Protocol for MANET*", International Journal of Power Control Signal and Computation,* vol. 3, no. 1, pp. 18-23, 2012.

[16] A. Ayyasamy and K. Venkatachalapathy., "Increased Throughput for Load based Channel Aware Routing in MANETs with Reusable Paths", *International Journal of Computer Applications,* vol. 40, no. 2, pp. 20-23, 2012.

[17] Kamal Kumar Chauhan and Amit Kumar Singh Sanger., "Securing Mobile Ad hoc Networks: Key Management and Routing", *International Journal on AdHoc Networking Systems,* vol. 2, no. 2, pp. 65-75, 2012.

[18] S. Sumathy and B.Upendra Kumar., "Secure Key Exchange And Encryption Mechanism For Group Communication in Wireless Adhoc Networks", *Journal on Applications of Graph Theory in Wireless Adhoc Networks and Sensor Network,* vol. 2, no. 1, pp. 9-16, 2010.

[19] N. Renugadevi and C.Mala., "Ternary Tree Based Group Key Agreement for Cognitive Radio MANETs", *Int.J. Computer Network and Information Security,* vol. 10, pp. 24-31, 2014.

[20] Deepak Puthal, Surya Nepal, Rajiv Ranjan, and Jinjun Chen., *"A Dynamic Key Length based Approach for Real-Time Security Verification of Big Sensing Data Stream",* ACM Transactions on Embedded Computing Systems (TECS) - Special Issue on LCETES, vol. 16, no. 2, pp. 93-108, 2017.

[21] Md. Golam Kaosar., "Routing Protocol Based Shared and Session Key Exchange Protocol for Wireless Mobile Ad-hoc Network", *Cryptography ePrint archieve,* pp. 229-235, 2011.

[22] Mohamed Eltoweissy, Mohammed Moharrum and Ravi Mukkamala., "Dynamic Key Management in Sensor Networks", IEEE Communications Magazine, pp. 122-130, 2006.

[23] Haowen Chan, Adrian Perrig and Dawn Son, "Random Key Pre-distribution Schemes for Sensor Networks*",* Research Showcase@CMU, pp. 1-17, 2003.

[24] K.C.Shyamala Bai, Dr.M.V.Satyanarayana and Dr. P.A. Vijaya., "Variable Size Block Encryption using Dynamic-key Mechanism (VBEDM)", *International Journal of Computer Applications,* vol. 27, no. 7, pp. 27-30, 2011.

[25] Zeenat Mahmood, J. L Rana and Prof. Ashish khare., "Symmetric Key Cryptography using Dynamic Key and Linear Congruential Generator (LCG)", *International Journal of Computer Applications,* vol.50, no. 19, pp. 7-11, 2012.

[26] Prakash, G., Vyas, B., & Kethu, V. R., "Secure & Efficient Audit Service Outsourcing For Data Integrity In Clouds", *International Journal of MC Square Scientific Research,* vol. 6, no. 1, pp. 5-60, 2014.

[27] Awadalla, M. H. A., "Heuristic Approach for Scheduling Dependent Real-Time Tasks", *Bulletin of Electrical Engineering and Informatics (BEEI),* vol. 4, no. 3, pp. 217-230, 2015.

[28] Manisha R. Dhage, Srikanth Vemuru, "Routing Design Issues in Hetrogeneous Wireless Sensor Network", *International Journal of Electrical and Computer Engineering (IJECE),* vol. 8, no. 2, 2018.

[29] Tamizharasi, A., Selvathai,j.j., Kavi priya, A., Maarlin, R., Harinetha, M., "Energy aware heuristic approach for cluster head selection in wireless sensor network", *Bulletin of Electrical Engineering and Informatics (BEEI),* vol. 6, no. 1, pp. 70-75, 2017.