RESEARCH ARTICLE OPEN ACCESS

A Comparative Study of Group Key Management in MANET

M. El-Bashary, A. Abdelhafez, W. Anis
Dept. of Comm. and Electronics Ain Shams University
Dept. of Comm. and Electronics Ain Shams University
Dept. of Comm. and Electronics Ain Shams University

Abstract
A Mobile Ad-Hoc Network (MANET) is a self organized network, with no fixed infrastructure, limited resources and limited physical security. Security in such an environment is an essential requirement. Key management is a salient element in MANET security. It is responsible for key generation, storage, distribution, updating, revocation, deleting, and archiving. Key management protocols are classified into symmetric, asymmetric, group, and hybrid. Group key management is a point of interest for researchers with the growing usage of mobile devices and the rising of multicast communication. This paper surveys different approaches in group key management schemes. A comparative study is demonstrated in terms of reliability, computational complexity, storage cost, communication overheads, pre-requirements, security levels, robustness, vulnerabilities, scalability, energy and mobility. Finally, the study concludes the pros and cons of each protocol.
Keywords: Group Key Management, MANET, security, multicast.

I. Introduction

Many of military and public safety applications based on MANET, as they can be rapidly deployed and configured. MANET suffers from dynamic topology, infrastructure-less, resources constraints, scalability, limited power, and limited physical security [1], [2]. Secure communications is needed in such environment [3]. Multicast transmission is an efficient communication mechanism for group oriented applications (such as video conferencing, video streaming, e-learning...) to save network resources [4]. So group key management is the most appropriate scheme in case of combination between MANET and multicast.

A group key should be shared among all members (nodes) in the group in order to multicast information. Encryption of information by group key lets the authorized users only that have the same group key to decrypt the information. But according to MANET characteristic, members of a group may be changed. If a new member joins the group, a new group key must be generated and distributed to all group members including the new member. This process prevents the new member to access the former information exchanged through the group, which is known as "Forward Security". The same process is taken when a member leaves the group as it has no rights to access the information anymore which is known as "Backward Security".

MANET can be exposed mainly to two types of attacks: passive attacks and active attacks [3]. A passive attack obtains data exchanged in the network without affecting the operation of the communication, while an active attack involves information interruption, modification, or fabrication. Examples of passive attacks are eavesdropping, traffic analysis and traffic monitoring. Examples of active attacks are: jamming, impersonating, modification, denial of service (DOS) and message replay.

Group key management protocols can be classified into centralized, decentralized, and distributed group key management [5]. In centralized group key management protocols there is a group key server (KS) which is responsible for group key distribution and updating. In decentralized group key management protocols the group is divided into subgroups. There is a group key shared among all group members, and every subgroup has a shared key among them known as Traffic Encryption Key (TEK). In this case there is a group key server (GK) for the group, and subgroup key server (SGK) for each subgroup. In distributed group key management protocols, which is also called key agreement, all members in the group cooperate to generate and distribute the traffic encryption key (TEK) for secure communications between them.

The centralized group key management protocols are easier to implement, but it is clearly not scalable since it suffers from the "1 affects n" phenomenon. The KS is considered being a bottleneck and a single point of failure. The decentralized group key management protocols need less bandwidth for key updating process. While the distributed group key management protocols are complicated and less scalable, but may be is the most appropriate approach for MANET as it eliminates the bottleneck and the single point of failure problems as well as "1 affects n" phenomenon. Updating keys methods can be done by three approaches as follows:

- *Member driven*: in which group key should be updated when a member joins or leaves the group in order to guarantee forward and backward security.
- *Time driven*: in which group key should be updated periodically at regular intervals.
- *Message driven*: it takes place only when a member wants to multicast a message.

The remainder of this paper is structured as follows:
Section 2: Centralized group key management protocols overview.
Section 3: Decentralized group key management protocols overview.
Section 4: Distributed group key management protocols overview.
Section 5: Discussion.
Section 6: Conclusion.

II. Centralized Group Key Management Protocols

In centralized group key management the generating, distributing, and updating the group key is being handled by one entity called Key Server (KS). This approach can be split into two categories; with keys pre-distribution and without key pre-distribution.

2.1. With Keys Pre-distribution

Nodes that form the group are initially configured offline before deployment. Each node is loaded by a set of keys in order to be able to decrypt multicast traffic, or to secure traffic encryption key (TEK) during rekeying process. Key pre-distribution is used in MANET because the lack of infrastructure, so it is not available to have central entity to handle the key distribution online. GKMPAN [6] and CKDS [7] are two protocols that follow this approach.

2.1.1. GKMPAN

GKMPAN assumes there is unavailability of key server (KS). It includes three main phases as follows:

a. Key pre-distribution:

Each group node "u" obtains offline before deployment, a subset (Iu) of "m" keys out of a pool of "l" keys. These keys are used as key encryption keys (KEKs). The key pre-distribution algorithm allows any node who knows another node's identifier "j" to determine its subset "Ij".

b. Authenticated node revocation:

When the key server (KS) decides to revoke a node, it broadcasts a revocation notification to the network, containing the identifier of the revoked node, and the non compromised key that is possessed by the maximum number of remaining nodes in the network.

c. Secure group key distribution:

KS generates and distributes a new group key. The key distribution process is achieved hop by hop, by encrypting the new group key with the pre-deployed KEKs. When a node is compromised and is revoked by the key server, its pre-deployed KEKs are also compromised. To face this problem when sending the new group key, KS determines the identifier of the non compromised KEK, shared with the maximum members of the multicast group. Then, it broadcasts a message containing the new group key encrypted with this chosen non compromised KEK. Group nodes who did not hold the KEK used to the encryption of the traffic encryption, it will receive this group key forwarded by their neighbors, encrypted with other non-compromised KEKs. So, the key server has only to deliver the new group key to its immediate neighbors, which forward it securely to their neighbors, in a hop by hop way.

d. Key update:

When the group nodes decrypt and authenticate the TEK, they update their subsets of pre-deployed KEKs, based on this TEK, and erase all the old KEKs. The compromised keys ki are also updated by the remaining members holding these keys, using a non compromised key km as follows:
ki ´ = fkm(ki), where f being a pseudo-random function.

2.1.2. Combinatorial Key Distribution Scheme (CKDS)

CKDS is another application level protocol that implements centralized key management with key pre-distribution. In this case KS is responsible for keys distribution and rekeying. The key distribution is based on an Exclusion Basis System (EBS) [8] associated with the Content Addressable Networks (CAN) [9]. Each node knows "k" keys (known keys) and does not know "m" keys (unknown keys). CAN is used to achieve a partition of all the nodes into an m-dimensional space. Thus, each node has a quadrant in the space, according to the unknown keys in the EBS scheme. If a node is compromised, the re-keying algorithm will start from the node which knows all the unknown keys of the compromised node. Thus, the new group keys can be spread via direct flooding along the m dimensions whose keys are not known by the compromised node, isolating this node in the re-keying procedure. In EBS matrix shown in table (1), if node U3 is compromised so K1, K2 and K5 are compromised as well. Any of the nodes U4, U7 or U10 can achieve the re-keying process because they know the unknown keys of U3 which are K3 and K4. Thus, the new group keys can be spread via direct flooding along the m dimensions whose keys are not known by the compromised node, isolating this node in the re-keying procedure.

	U 1	U 2	U 3	U 4	U 5	U 6	U 7	U 8	U 9	U1 0
K 1	1	1	1	1	1	1	0	0	0	0
K 2	1	1	1	0	0	0	1	1	1	0
K 3	1	0	0	1	1	0	1	1	0	1
K 4	0	1	0	1	0	1	1	0	1	1
K 5	0	0	1	0	1	1	0	1	1	1

Table (1): EBS Matrix

2.2. Without Keys Pre-distribution

Key generation and distribution is handled online by the KS. Kaya et al. [10] and Lazos-Poovendram (L-P) [11] are two protocols that follow this approach.

2.2.1. Kaya et al. Protocol

Kaya et al. proposes a group key management protocol, which is efficient against mobility, non-reliability and multi-hop overheads. Certification service is assumed to ensure access control and revocation of malicious members. Each member should obtain a security certification from a Trusted Third Party (TTP) before joining the group. KS multicasts a revocation list periodically to group members' that includes revoked certifications. Group members store this list, check and authenticate the new joining members. New node can join the multicast group through the closest neighbor node using the Global Positioning System (GPS) information. Join request was broadcasted in limited range to reach any group member, while the response from the neighbor members was sent in anycast mode. This can lead to optimized key distribution according to construction of multicast tree with shortest paths. This can reduce multi-hop, complexity and communications costs challenges in MANET. Data integrity is carried out by Timed Efficient Stream Loss-tolerant Authentication (TESLA) [12] approach which needs synchronization between source and destinations. Synchronization is expensive in MANET environmental.

2.2.2. L-P Protocol

L-P is another protocol that follows the same approach. It improves key distribution of Logical Key Hierarchy (LKH) [13] using geographical localization of the group members based on GPS, optimizing energy consumption. Simply, members who are close to each other can receive a multicast data through the same path. The K-means [14] clustering algorithm is used to form groups with strong correlation. It assigns the group members to a fixed number of clusters randomly, and then changes the membership of the clusters by maximizing the correlation between the members of each cluster. The algorithm iterates this process until the assignment of the members to the clusters does not change, this means that clusters have the best geographical correlation.

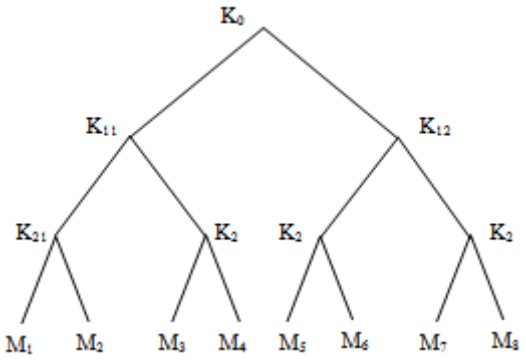

Figure (1): Key distribution tree based in the K-means algorithm

K-means is implemented by the following steps:

a. Assign all group members in one cluster.
b. Divide the cluster into two sub-clusters by K-means algorithm.
c. Balance the number of members per cluster.
d. Iterate steps b, c until each cluster has one or two members only.
e. Merge clusters of one member.
f. Map the cluster hierarchy into the logical hierarchy of LKH distribution.
g. The final cluster tree will be as shown in figure (1).

2.2.1. Other Protocols

Logical Key Hierarchy for Wireless sensor network (LKHW) protocol [15] is a directed diffusion process with LKH tree distribution. It provides good efficiency with respect to energy resources.

III. Decentralized Group Key Management Protocols

The decentralized approach divides the multicast group into sub-groups or clusters; each sub-group is managed by a cluster head (CH) responsible for the key management for its sub-group (cluster). Two categories of protocols adopt this approach, local TEK and common TEK. In local TEK key management protocol the multicast group is split into clusters. One of the nodes in each cluster acts as cluster head (CH), the rest of the nodes are members in the cluster. Multicast communication can take place through two types of keys. The cluster group key (CGK) is shared key between CH and its members and used to secure intra-cluster traffic. While key encryption key (KEK) is shared by CH and each cluster member, and used to encrypt CGK and distribute it to each cluster member. Inter-cluster

traffic is limited to CHs only. In common TEK no intermediate encryption and decryption of multicast traffic by LC, which is considered to be an advantage for a limited storage, processing, and power limitations in ad hoc environment. It also minimize "1 affects n" phenomenon.

3.1. Enhanced BAAL Protocol

Enhanced BAAL [16] is a local TEK protocol that defines the global controller (GC), local controller (LC), and cluster member (CM). GC is the source of the multicast group, and is responsible for the generation, distribution and periodic renewal of TEK. GC sends a request to a defined number of threshold cryptography servers, which answer by sending their contributions. Then, the GC combines these contributions to constitute the TEK, and distributes it to all its group members. LC is one of GC members which manage a local TEK with its members. It is responsible for forwarding the multicast flow sent by the multicast source to all its local members. This approach tends to attenuate the "1 affects n" phenomenon. However, the intermediate operations of encryption and decryption are challenges in an ad hoc environment, with limited storage and computing power.

3.2. BALADE Protocol

BALADE [17] is a common TEK protocol in which the multicast group is divided dynamically into clusters. Each cluster is managed by a local controller (LC) which shares with its local members a local cluster key KEK_{CSG}. The multicast flow is encrypted by the source with TEK and sent in multicast to all the group members. The source of the group and the local controllers form a multicast group called Group of Local Controllers (GLCs) and share beforehand a session key called KEK_{CCL}. In case of authentication success, the parent controller authorizes the LC to join the GLCs and sends Access Control List (ACL) and revocation list to it. Each new local controller has to join this group and receive the session key KEK_{CCL} from the source of the group, encrypted with its public key. The split process is achieved using Optimized Multicast Cluster Tree (OMCT) algorithm. The multicast source sends the TEK to the group of the LCs, encrypted with KEK_{CCL}. The LCs forward the TEK to their local members, encrypted with their respective local cluster key. The centralized group key management protocols are easier to implement, but it is clearly not scalable since it suffers from the "1 affects n" phenomenon.

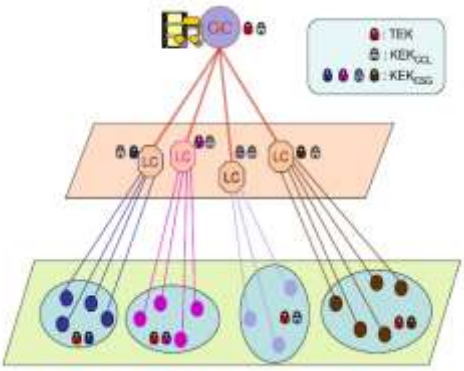

Figure (2): The group key generation and distribution in BALADE.

The KS is considered being a bottleneck and a single point of failure. The decentralized group key management protocols need less bandwidth for key updating process. While the distributed group key management protocols are complicated and less scalable, but may be is the most appropriate approach for MANET as it eliminates the bottleneck and the single point of failure problems as well as "1 affects n" phenomenon.

3.3 Other Protocols

Vardharajan, Hitchens, and Shakaran (VHS) protocol [18] operates within Near-Term Digital Radio (NTDR) architecture, in which the architecture composes of set of clusters and each set of cluster contains cluster head. This protocol provides efficient use in terms of mobility environment.

IV. Distributed Group Key Management Protocols

In this approach all members in the multicast group should cooperate to generate and distribute encryption key for secure communications.

4.1. Chiang-Huang (C-H) Protocol

Chiang-Huang (C-H) [19] proposes a group key management protocol for MANETs based on GPS information and on Group Diffie-Hellman (GDH) group key exchange protocol [20-21]. During protocol initialization, each node in the ad hoc network floods its GPS information and its public key to all others nodes with no need for Certificate authority (CA). Based on GPS information, each node has the capability to build up network topology. When a node needs to send a multicast data, it computes the shortest path through the multicast tree according to Prufer algorithm [19]. This node generates the group key as a combination of group members' public keys, and then distributes it to all multicast group members. The GDH key distribution graph using the Prufer algorithm is defines two types of nodes are defined, leaf nodes (u-nodes) representing the multicast users' nodes, and the k-

nodes representing keys. The root of the key graph is called k_p-node. U is the set of multicast users, K is the set of keys, and P is the Prufer-key (group key). Figure (3) illustrates the key graph.

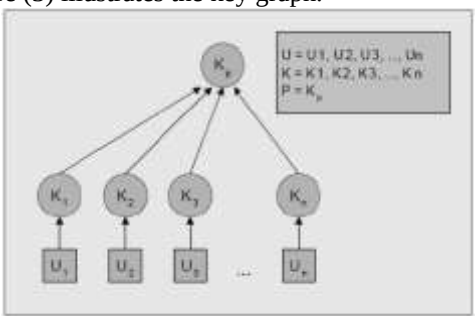

Figure (3): A key Graph for C-H protocol

Mobility Based Key Management (MBKM) [22] protocol is the approach based on link quality and reputation of nodes to identify them as strong and weak nodes in a distributed tree-manner. The topology configuration is a hierarchical tree distribution with periodic flooding (rekeying process) of control messages. The computations of the protocol depend on the reputation list management; multicast data encrypted and decrypted, and message hashing. The storage cost depends on GDH [21] tree key. The routing of all messages is done by cluster heads which are based on the reputation index. The constrains of this protocol are the clustering algorithm needed for the construction, the stability threshold needed for the environment, and the rekeying time threshold to determine the threshold intervals of weak and strong nodes. This protocol guarantees authentication, access control, data confidentiality, and data integrity. It is robust against faulty nodes but the main weakness of the construction comes from the cluster heads. It provides good scalability and efficiency for mobility environments.

4.1. Other protocols

There are many distributed protocols such as Ingmarsson, Tang, and Wang (ING) [21] and CLIQUES (CLIQ) [23], where such this two protocols are the extensions of the generic two-party Diffie and Hellman (D-H) protocol [20] to n-participants with a logical ordering construction. Another recent protocol, which its issue is different from the previous two protocols, is Hierarchical, Simple, Efficient, and Scalable Group Key Management (HSESGK) Protocol [24]. This scheme, which is based on clustering algorithm and needs certificate authority, is the evolved version of the Simple and Efficient Group Key (SEGK) scheme [25]. It provides good scalability and has efficient use under mobile conditions.

V. Discussion

This section compares and analyzes the differences among group key management protocols discussed above. The comparison will include the challenges for multicast communications in MANET environment such as main characteristics, reliability, computational complexity, storage cost, communication overheads, pre-requirements, security levels, robustness, vulnerabilities, scalability, and efficiency.

Main characteristics highlight the main idea of protocol construction. Reliability reflects the flexibility of network topology. Computational complexity is according to the multiple encryption and decryption processes of traffic flow. In the storage cost parameter, the key management scheme should have minimum number of stored keys. Communication overheads address the maximum size of key management message. Pre-requirements define the constraints for protocol construction. Security levels verify the security services; authentication, access control, data confidentiality, data integrity …etc. Robustness measures the immunity of the protocol design against faulty nodes. Vulnerabilities demonstrate the critical weakness of the network entities. Scalability is the ability of the key management scheme to seamlessly scale to network size. Efficiency is the ability to save energy resources and copes with node mobility.

5.1. Centralized Group Key Management Schemes

The main characteristic of GKMPAN protocol that it should be initially configured offline before deployment. GKMPAN assumes the unavailability of KS. GKMPAN exploits the multi-hop property of the ad hoc networks. GKMPAN generates the TEK then distribute it to the neighbor nodes encrypted with non compromised KEK to its immediate neighbors. Neighbors forward the TEK securely to their neighbors based on the multi-hop property of the ad hoc networks achieving reliability. TEK is encrypted and decrypted more than once to reach all the network nodes. TEK is distributed securely using pre-deployed KEKs. Increasing the number of pre-deployed keys leads to increase the number of logical paths between nodes, but this will increase the storage cost as well. Increasing the number of the KEK pool "l" with small number of pre-deployed KEKs results in enhancement of security level. Using TESLA authentication of a broadcast message contains the new group key increases the computation complexity. TESLA authentication needs synchronization between network nodes which is difficult to be implemented in ad hoc environment. The multihop awareness of GKMPAN decreases the communication overheads required for routing within the network. Security level is verified by a number of

procedures including verification of new TEK, updating of pre-deployed KEKs, and revocation of compromised nodes. The main vulnerability is the KS as a single point of failure. Scalability of centralized scheme is very limited according to the centralized environment. But GKMPAN can show more scalability on the expense of storage requirements for pre-distributed keys. GKMPAN achieves fair efficiency in terms of energy resources and node mobility.

CKDS is an application level protocol based on EBS matrix and CAN configuration for securing multicast communications in ad hoc networks. CAN is used to achieve a partition of all the nodes into an m-dimensional space. Rekeying algorithm started from the diagonal node in the partitioned space which knows all unknown keys of the compromised node. TEK is encrypted and decrypted in m-dimensional space according to CAN and EBS which represent a computation complexity. The storage cost increases as the number of pre-deployed KEKs increases. The multihop awareness of CKDS decreases the communication overheads required for routing within the network. Security level is ensured by node revocation and data confidentiality. Multicast data is encrypted and decrypted once by the communication parties only, no intermediate encryption/decryption operation. Global Controller (GC) is the main vulnerability in the network as a single point of failure. Scalability of CKDS is better than any other centralized scheme like LKHW or GKMPAN.

K-P scheme has no need to keys pre-deployment. It is characterized by exploiting of nodes' localization for network optimization. The GPS information is used by new nodes to join the group through closest neighbor. This information helps in reduction of communication overheads and achieving the optimization of key distribution in a multicast tree. Data integrity is maintained by TESLA protocol that needs synchronization between nodes. Synchronization has an expensive cost in ad hoc environment. Certification service is used to ensure authentication and access control. Every node should get a certificate from a CA offline before joining the group. Every node should store its certification and the revocation list as well. Storage cost is a function of TESLA buffering as well. Scalability is not addressed in this protocol. Updating of revocation list is considered to be the vulnerability in this protocol. A better efficiency is achieved in terms of energy resources and mobility awareness.

L-P protocol enhances the LKH protocol by using the geographical information of the nodes. So that members which are close to each other, can potentially be reached by a broadcast message, or can use the same path to receive the multicast data optimizing the communication overheads and energy resources as well. The multicast flow is decrypted by communication parties with no need for intermediate encryption and decryption processes achieving data confidentiality and less computation complexity. It uses a hierarchal tree distribution technique in the multicast group by using K-means algorithm. Vulnerability of L-P scheme is the KS as all the types of centralized approach.

5.2. De-centralized Group Key Management Schemes

The E-BAAL protocol is mainly based on threshold cryptography, using a hierarchical tree distribution. The rekeying procedure is based on Adaptive Key Management Protocol (AKMP). Multiple encryption and decryption of multicast traffic increases the computation complexity, communication overheads, and the storage cost. On the other hand, E-BAAL represents good security levels such as authentication, access control, and data confidentiality. Robustness, fair scalability and fair efficiency with respect to mobility are provided.
BALADE protocol enhances the deficiencies in E-BAAL. It avoids multiple encryption and decryption of multicast traffic by using common TEK for encryption multicast data within the group. Multiple encryption and decryption is only applied to distribute TEK securely using KEKs. BALADE is efficient protocol in terms of energy resources and mobility environment.

5.3. Distributed Group Key Management Schemes

C-H protocol is based on GPS information and the GDH key agreement protocol. Flooding of GPS information and public keys increases the communication overheads, which is very expensive in ad hoc environment. Each member can build the network topology using Prufer algorithm. No need for intermediate encryption and decryption processes of the multicast traffic achieves less computation complexity. The price is high storage cost to meet Prufer sequence requirements. Flooding of GPS information and executing Prufer algorithm restrict the scalability of the network. The protocol suffers from a poor efficiency in terms of energy resources.
ING and CLIQ protocols have poor scalability, efficiency and security levels. Computation complexity is dependent on the number of nodes in the group. Traffic encryption and decryption increases the storage cost and communication overheads as well. Meanwhile, HSESGK and MBKM schemes provide robustness, security, mobility and good scalability.

5.4. Comparison of the Group Key Management Protocols

In this section, the comparison of the group key management protocols is studied. Tables (1), (2), and (3) illustrate the comparative studies of most

common, important, and recent schemes for centralized, de-centralized and distributed group key managements respectively.

VI. Conclusion

In this paper, the state of the art within group key management for MANETs is surveyed. A set of evaluation criteria for MANETs group key management schemes are defined. Each category of group key management is evaluated and compared according to the identified criteria. In summary, based on evaluation criteria a comparative study is conducted to show the advantages and disadvantages of the centralized, de-centralized and distributed group key management protocols for MANETs.
Generally there is no one single protocol in this paper that is effective for all MANET scenarios. The application must be taken into consideration at the current state of the art. The optimal combination of energy, mobility and security should be sought in future key-management proposals.

References

[1.] A. Hegland, E. Winjum, S. Mjolsnes, C. Rong, O. Kure, and P. Spilling, "A survey of key management in ad hoc networks," IEEE Communications Surveys, pp. 48-66, 2006.
[2.] M.Yonis and S. Ozer, "Wireless ad hoc networks: technologies and challenges," Wireless Communications and Mobile Computing, pp. 889-892, 2006.
[3.] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," ACM Computing Surveys, pp. 309-329, Sep. 2003.
[4.] L. Junhai, X. Liu, and Y. Danxia, "Research on multicast routing protocols for mobile ad –hoc networks," Computer Networks, pp. 988-997, 2008.
[5.] A. Renuka and K. Shet, "Hierarchical approach for key management in mobile ad hoc networks," International Journal of Computer and Information Security (IJCSIS), pp. 87-95, 2009.
[6.] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: an efficient group rekeying scheme for secure multicast in ad hoc networks," Technical Report, 2004.
[7.] M. Moharrum, R. Mukkalamala, and M. Eltoweissy, "Ckds: an efficient combinatorial key distribution scheme for wireless ad hoc networks," IEEE International Conference on Performance, Computing, and Communications (IPCCC), pp. 631-636, 2004.
[8.] L. Morales, I. Sudborough, M. Eltoweissy, and M. Heydari, "Combinatorial optimization of multicast key management," IEEE International Conference on System Sciences, 2003.
[9.] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker, "A scalable content-addressable network," Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM 01), 2001.
[10.] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz, "Secure multicast groups on Ad Hoc networks," in Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 94-102, 2003.
[11.] L. Lazos and R. Poovendram, "Energy-aware secure multicast communication in Ad Hoc networks using geographical location information," in IEEE International Conference on Acoustics Speech and Signal Processing, pp. 201-204, 2003.
[12.] A. Perrig, R. Canetti, D. Tygar, and D. Song, ''The TESLA broadcast authentication protocol," RSA Laboratories Cryptobytes, vol. 5, no. 2, pp. 2-13, 2002.
[13.] C. Wong, M. Gouda, and S. Lam, "secure group communications using key graphs," in ACM SIGCOMM, pp. 68-79, 1998.
[14.] J. B. MacQueen,' 'Some methods for classification Band analysis of multivariate observations," in Proceedings of 5-th Berkeley Symposium on Mathematical Statistics and Probability, pp. 281-297, 1967.
[15.] R. D. Pietro, L. Mancini, Y. Law, D. Etalle, and P. Havinga, "LKHW: A directed diffusion based secure multicast scheme for wireless sensor networks," in International Conference on Parallel Processing Workshops (ICPPW'03), pp. 397-406, Oct. 2003.
[16.] M. S. Bouassida, I. Chrisment, and O. Festor, "An enhanced hybrid key management protocol for secure multicast in Ad Hoc networks," in Networking 2004, Third International IFIP TC6 Networking Conference, LNCS 3042, pp. 725-742, Springer, May 2004.
[17.] M. S. Bouassida, I. Chrisment, and O. Festor, "Group Key Management in MANETs" International Journal of Network Security, pp. 67–79, Jan. 2008.
[18.] V. Varadharajan, M. Hitchens, and R. Shankaran, "Securing NTDR Ad-Hoc Networks," in IASTED International Conference on Parallel and Distributed Computing and Systems 2001, pp. 593-598, Aug. 2001.

[19.] T. Chiang and Y. Huang, "Group keys and the multicast security in Ad Hoc networks," in Proceedings of the 2003 International Conference on Parallel Processing Workshops (ICPP 2003 Workshops), pp. 385, 2003.
[20.] W. Daffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, pp. 644-654, Nov. 1976.
[21.] I. Ingemarson, D. Tang, and C. Wong, "A conference key distribution system," IEEE Transactions on Information Theory, pp. 714-720, Sep. 1982.
[22.] B. Madhusudhanan, S. Chitra, and C. Rajan, "Mobility based key management technique for multicast security in mobile ad hoc networks," The Scientific World Journal, 10 pages, 2015.
[23.] M. Steiner, G. Tsudik, and M. Waidner, "CLIQUES: A new approach to Group Key Agreement," Proceedings of ICDCS'98, 1998.
[24.] A. EL-Sayed, A new hierarchical group key management based on clustering scheme for mobile ad hoc networks," International Journal of Advanced Computer Science and Applications, pp. 208-219, 2014.
[25.] B. Wu, J. Wu, and Y. Dong, "An efficient group key management scheme for mobile ad hoc network," International Journal of Security and Networks, pp. 217-226, 2208.

	GKMPAN [6]	**CKDS [7]**	**Kaya et al. [10]**	**L-P [11]**	**LKHW [15]**
Main Characteristics	Identification of non compromised KEKs by KS	Key distribution based on EBS and CAN	Periodic signature of certificate revocation list	Geographical information of nodes are used for routing	Direct diffusion process with LKH tree distribution
Reliability	Group member share the same TEK distributed via pre-deployed keys	m-dimensional space flooding process	Hierarchal tree distribution	Hierarchal tree distribution	Hierarchal tree distribution
Computation complexity	TEK encryption and decryption, and TESLA procedure	TEK encryption and decryption in m-dimensional space according to EBS and CAN	Multicast data encryption and decryption, and TESLA procedure	Multicast data encryption and decryption in K-means clustering manner	Message hashing and key generation based on direct diffusion manner
Storage Cost	Pre-distributed keys and TESLA buffering	Pre-distribution keys and EBS matrix	Revocation list, certificates, and TESLA buffering	LKH tree key distribution	LKH tree key distribution
Communication Overheads	Running routing protocol with one-hop neighbors	Running m-dimensional routing protocol with one-hop neighbors only	Optimization of multicast tree distribution	Group initialization based on LKH distribution	LKH distribution
Pre-requirements	Key pre-distribution and synchronization	Key pre-distribution, EBS matrix with CAN, and GC	GPS, CA, and synchronization	GPS and K-means algorithm	Direct diffusion algorithm
Security Levels	Node revocation and data confidentiality	Node revocation and data confidentiality	Authentication, access control, data confidentiality and integrity	Data confidentiality	Authentication, data confidentiality, and integrity
Robustness	Yes	Yes	Yes (better than both GKMPAN and CKDS)	Yes	Yes
Vulnerabilities	KS	GC	Revocation list updating	Multicast source	Multicast source
Scalability	Fair	Good	Poor	Poor	Poor
Efficiency	Fair	Fair	Good in terms of mobility	Good in terms of energy resources	Good in terms of energy resources

Table (1): Comparison of Centralized Protocols.

	E-BAAL [16]	**VHS [18]**	**BALADE [17]**
Main Characteristics	Group entity holds public and private key generated by the server nodes of the threshold cryptography	The protocol operates within NTDR architecture, in which each set of cluster contains cluster head (CH)	Division of multicast group into clusters and common TEK
Reliability	Hierarchical tree distribution and rekeying process based on AKMP	NTDR architecture	Hierarchical tree distribution and rekeying based on OMCT dynamic clustering algorithm
Computation complexity	Multiple encryption and decryption of multicast traffic, and TEKs encryption and decryption by LCs	Multicast data encryption and decryption by CHs	Multiple encryption and decryption of TEK only
Storage Cost	Public and private keys, and multicast traffic encryption and decryption by LCs	Multicast data encryption and decryption by CHs	KEK per cluster, revocation list, and ACL
Communication Overheads	Key generation messages and notification to LCs	Routing of all messages by CHs	OMCT group distribution
Pre-requirements	Clustering algorithm and threshold cryptography	Clustering algorithm and certificates	Clustering formation algorithm and GPS
Security Levels	Authentication, access control, and Data confidentiality	Data confidentiality	Data confidentiality, integrity, access control, and authentication
Robustness	Yes	Yes	Yes
Vulnerabilities	GC	CHs	GC
Scalability	Fair	Fair	Fair
Efficiency	Poor with respect to energy resources, and fair with respect to mobility	Fair with respect to mobility	Fair with respect to energy resources and mobility

Table (2): Comparison of Decentralized Protocols.

	ING [21]	**CLIQ [23]**	**C-H [19]**	**HSESGK [24]**	**MBKM [22]**
Main Characteristics	Extension of two-party DH protocol to n-parties using logical ring of nodes	Changes of group from group controller by extending DH protocol dynamically	GDH protocol and GPS measures	Group members deduce the group key in a hierarchical distributed manner	Hierarchical tree distribution, and link quality and node reputation determine node identification
Reliability	Ring ordering	Node ordering	Hierarchical tree distribution based on Prufer algorithm	Hierarchical tree distribution with periodic flooding of control messages	Hierarchical tree distribution with periodic flooding of control messages
Computation complexity	Grows exponentially to the number of nodes	Grows exponentially to the number of nodes	Public key computation and Prufer sequence	multicast traffic encryption and decryption by CHs	Reputation list management, multicast traffic encryption and decryption, and message hashing.
Storage Cost	Traffic encryption and decryption	Traffic encryption and decryption	Prufer sequence	multicast traffic encryption and decryption	GDH protocol

Communication Overheads	Grows exponentially to the number of nodes and logical ring of one-hop neighbors only	Grows exponentially to the number of nodes, logical ring of one-hop neighbors only	Flooding of the GPS localization and the public keys	Routing of all messages by CHs and periodic flooding of control messages	Routing of all messages by CHs based on reputation index (RI)
Pre-requirements	Key pre-distribution	Key pre-distribution	GPS and GDH protocol	Clustering algorithm and CA	Clustering algorithm, stability threshold, and rekeying time threshold
Security Levels	NO	NO	Data confidentiality	Data confidentiality, integrity, access control, and authentication	Data confidentiality, integrity, access control, and authentication
Robustness	NO	NO	Yes	Yes	Yes
Vulnerabilities	Ring ordering and man in the middle (MIM)	Ordering, GC, and MIM	GPS flooding and high overheads	CHs	CHs
Scalability	Poor	Poor	Poor	Good	Good
Efficiency	Poor	Poor	Poor	Good with respect to mobility environment	Good with respect to mobility environment

Table (3): Comparison of Distributed Protocols