Journal of Computer Science 9 (10): 1260-1266, 2013
ISSN: 1549-3636

doi:10.3844/jcssp.2013.1260.1266 Published Online 9 (10) 2013 (http://www.thescipub.com/jcs.toc)

AN EFFICIENT AUTONOMOUS KEY MANAGEMENT WITH REDUCED COMMUNICATION/COMPUTATION COSTS IN MOBILE AD HOC NETWORK

[1]M. Devi and [2]S. Chenthur Pandian

[1]Departmen of MCA, Selvam College of Technology, Namakkal, Tamilnadu, India
[2]SNS College of Technology, Coimbatore, Tamilnadu, India

Received 2013-06-13, Revised 2013-08-07; Accepted 2013-08-21

ABSTRACT

A primary concern in Mobile Ad Hoc Networks (MANETs) is security. Secret sharing is an effective way to distribute a secret among n parties, where each party holds one piece of the secret. A number of key management schemes have been proposed for MANETs. However the secret sharing to control key hierarchy needs larger message transmission costs in many techniques. Existing research in key management can only handle very limited number of nodes and are inefficient, insecure, or unreliable when the nodes increases. Here this study modifies Autonomous key management scheme is proposed to address both for security and efficiency for key management in Mobile Ad hoc Network (MANET). It also reduces communication and computational cost in Ad-Hoc Network and works for large number of nodes.

Keywords: Mobile Adhoc Network, Key Management, Autonomous Key Management, IDentity-Based (ID-Based) Public Key System, Trusted Authority

1. INTRODUCTION

In wireless networking MANET could be a distinctive kind consisting of a group of nodes capable to communicate with one another while not facilitate from a network infrastructure. Applications of MANETs embody the battlefield applications, rescue works, in addition as civilian applications like an out of doors meeting, or a billboard hoc classroom. Providing security services to MANETs, has been a difficult task for several years and has been under analysis. Answer for numerous sorts of attacks in MANETs has been a exhortation amongst researchers as a result of MANETs applications are extended for the employment in military applications, emergency rescue operations, in confidential video conferencing.

A MANET is an automated network that is totally dynamic and distributed in nature. The functionalities of each node are alike wherever in identification of an attacker or malicious nodes amongst the network could be a difficult task. Maintaining the security for multicast routing in MANETs is equally vital. There are several security protocols under the practicality of multicast has been designed. However these protocols are at risk of numerous sorts of attacks on MANETs like flooding, black hole, wormhole. There has been several works revealed within the literature concerning their attacks and also the answer for the attacks. With the increasing variety of applications to harness the benefits of ad hoc Networks, additional considerations arise for security problems in MANETs (Rafat and Haque, 2009).

To ensure communication between network devices, MANETs use the radio link. This enables a malicious node to infiltrate easily to disrupt the network. To stop such behavior, a cryptographic authentification system ought to be established. However, the authentification system ought to include a trustworthy entity which will manage the cryptographic keys. Efficient management of keys, or digital certificates holding the keys, is one in all the key factors for the productive wide-spread

Corresponding Author: M. Devi, Departmen of MCA, Selvam College of Technology, Namakkal, Tamilnadu, India

deployment of cryptographic keys. Public Key Infrastructure (PKI), an infrastructure for managing digital certificates, was introduced for this purpose.

Hybrid approach for key management is a promising research direction for scalable MANETs. In this hybrid key management approach through using the zone concept instead of using the clustering. Finding a more efficient way for creating the public key without losing the ability of creating certificates in a distributed manner is considered one way to improve their schema (Khdour and Aref, 2012).

1.1. Related Works

The number of applications that utilizes the Ad-Hoc Networks has magnified step by step over the years. Hence, it's necessary to contemplate the security issue of Ad-Hoc Networks. Numbers of research have contributed several security systems to certify the MANETs. This section of the survey primarily focuses on earlier contributed research works within the field of security to MANETs through cryptographic techniques like Distributed Key generation, Pair-wise key generation.

Blakley (1997) and Shamir (1997) invented two (k, n) threshold-based Secret Sharing Schemes (SSS) for $k \leq n$. The overall idea behind a "secret sharing" is to distribute a secret (e.g., encryption/decryption key) to totally different participants so any k participants will reconstruct the secret and any (k-1) or fewer participants cannot reveal the key. In different words, there's a delicate distinction between unqualified groups cannot obtain any information regarding the key and unqualified group cannot reconstruct the key. For instance, although knowing information regarding the key is an excellent variety, it's still quite troublesome to see the precise value of the key.

Wu *et al*. (2008) Group key management is one of the basic building blocks in collaborative and group-oriented applications in Mobile Ad Hoc Networks (MANETs). Group key establishment involves creating and distributing a common secret for all group members. Though key management for a large and dynamic group is a difficult problem because of scalability and security. Slide changes in the membership requires the group key to be refreshed to ensure backward and forward secrecy (Khdour and Aref, 2012) uses Zone Routing Protocol (ZRP). In this model for each mobile node zone is defined. Some pre-defined number is allocated to each mobile node which depends on the distance in hops. Symmetric key management is used by mobile node only for intra or inside r zone (zone radius). Without depends on clustering mobile node uses asymmetric key management for inter-zone security. Provides efficient way to making the public key without losing the capability of making the certificates.

Francis *et al*. (2013) MANET is a self-configuring network of mobile nodes connected by wireless links to form an arbitrary topology without the use of existing infrastructure. Because of the nature of Unreliable Wireless medium Data Transfer is a major Problem in MANET and it lacks Security and Reliability of Data. For secure Data transmission wireless networks Cryptographic techniques are commonly used. Most cryptographic techniques, such as symmetric and asymmetric cryptography it is often involved in the use of cryptographic keys. Though all the techniques in cryptographic will be useless if the key management is weak. central component in MANET security is the Key management. Numerous key management schemes have been proposed for MANET.

Raghavendran *et al*. (2013) MANETs have revolutionized the field of networking with increasing number of their commercial and military applications. For this security is now an essential requirement for these applications. Thopugh there are some limitations of the dynamic and infrastructure-less nature of MANETs impose major difficulties in establishing a secure framework suitable for such services. MANETs security is a dynamic area of research. Majority traditional routing protocols proposed for MANETs are focused on routing only not on the security aspects. Wired networks and wireless networks also required for security purpose. Unlike the wired networksthere are some dedicated routers are serverd for control the network in MANETs nodes act both as terminals and also as routers for other nodes. One of the famous mechanism to satisfy the security requirements is the Group Key Management in which the group key is to be shared by each group communication participant. To establish and manage the group key efficiently imposes new challenges especially in infrastructure less MANETs.

1.2. Existing Method

Autonomous Key Management (AKM) is planned for the Mobile Adhoc Network (MANET) with an oversized variety of nodes, supported a data structure to supply flexibility and adaptively. In AKM, It tends to assume that every real node joins and leaves the network willy-nilly. Therefore, thanks to the ranked nature of AKM, for a virtual node, the upper level it belongs to, the lower is that the likelihood of occurrences of region-based operations (e.g., "Merge" and "Partition") involving this virtual node. In different words, the upper

levels of the data structure stay comparatively static, in spite of the very fact that in painter rock bottom level of AKM (i.e., those real nodes) is very dynamic.

Additionally, another main advantage of AKM is the flexibility of its structure. Each region can determine its own size and the threshold of secret sharing, as long as it obeys the following rule: its RTC should be no less than GTC. The flexibility of the threshold parameter is very desirable, since in some cases different regions of the MANET may face risks of different intensities. Thus, the threshold should not be set to be globally uniform. Moreover, such property is very useful in balancing the security and efficiency requirements. Together with this property, it can set appropriate RTCs so that the region-based operations are limited in lower levels.AKM includes six node-based/region-based operations from node joining, region partitioning, to node leaving. AKM runs dynamically with continuous node joining/leaves.

In the earlier system of AKM which is based on the hierarchical structure and secret sharing to distribute cryptographic keys and provide certification services. In order to be employed in MANET, AKM is designed with several characteristics which are different from previous hierarchical key management schemes. First, the hierarchical structure of AKM is a logical tree, in which all the leaf nodes represent real wireless devices, while all the branch nodes only exist logically. Once AKM is in operation, each real node holds a secret share which is used cooperatively with other nodes to maintain distributed key management services, such as assigning a secret share or a certificate to a newly-joined node. At the algorithm level, proposed system of two algorithms, which are based on threshold cryptography and are independent from AKM. Both algorithms can resist active attacks. Given that there is no communication error, our first algorithm can assign a certificate within one round with help from a group of 2k-1 nodes, in spite of active attacks. In contrast, the second algorithm need help from only k nodes, although it may need more than one round to assign a certificate. Here, one round is defined to be the whole procedure that begins from a node requesting to be assigned a new certificate or renew its certificate to the combination and validation process of the certificate assigned or renewed (Zhu *et al*., 2005).

1.3. Proposed AKM

AKM includes six node-based/region-based operations from node joining, region partitioning, to node leaving. AKM runs dynamically with continuous node joining/leaves:

- All leaves in the hierarchy of AKM are Real nodes. Each real node i has its own secret key SK_i and $PK_i = g^{Ski} \pmod p$
- The non-leaf nodes are Virtual nodes and their secret keys are generated directly/indirectly from real nodes through some region-based operations
- A tree with node A as root is called Region A. For example, region A has virtual nodes B1, B2 and real nodes C1,1, C1,2, C1,3, C2,1, C2,2, C2,3 and C2,4. The number of the nodes that know the secret of the region is Overall Region Size (ORS). Finally, this study computes the Regional Trust Coefficient (RTC) --- the ratio of the threshold to ORS evaluating how secure the region is. The AKM sets a Global Trust Coefficient (GTC) as a lower bound of all the RTC

The six operations are update, join, leave, merge, partition and expansion. The operations are described below.

1.4. Update Operation

Operation “update” prevents any intruders from compromising the secret and the AKM updates keys periodically. First, the region with (n, t)-threshold has to select t nodes and each node is indicated as node i $\in \{1, \ldots, t\}$.

Each node i generates update share Si, j ($1 \leq j \leq n$) of key 0. It selects random numbers xj ($1 \leq j \leq n$) and rd ($1 \leq d \leq i-1$) to compute coefficients ad = (rd | 0) ($1 \leq d \leq t-1$):

$$S_{i,j} = a(x_j) = \sum_{r=0}^{t-1} a_r (x_j)^r \pmod p, \text{ for } 1 \leq j \leq n$$

Distributes Si, j to node $j \in \{1 \ldots n\}$. When node j receives the update shares distributed from other t nodes in the region, it computes a new share:

$$S_j^{'} = S_j \sum_{i=1}^{t} S_{i,j} \pmod q$$

The previous section mentions that AKM with six-region based Operations can manage its secret sharing hierarchical structure. The operations cover all possible region changes from node joining to leaving.

1.5. “Join” Operation

Operation “Join” is used when a node i want to join into a (t, n) threshold region. It sends a request to node j $\in \{1, \ldots, t\}$ in the region. Receiving the request, node j

checks its Certificate Revoking List (CRL) first. If node j accepts the request, it computes a partial share S'j of node i:

$$S_j^{'} = S_j l_j(i) + \Delta_j \pmod q$$

Where: $L_j(i) = \prod_{r=1, r\neq j}^{t} \frac{ID_i - ID_r}{ID_j} \frac{ID_r}{ID_r} \pmod q$

$$\Delta_j = \sum_{r=1, r\neq j}^{t} \sigma(j-r), S_{j,r}$$

That S j, r is a number which pairs of nodes (j, r) $\in \{1 \leq j \leq t, 1 \leq r \leq t\}$.

After receiving all partial shares, node i generates its secret share Si:

$$S_i = \sum_{j=1}^{t} S_j^{'} = \sum_{j=1}^{t} S_j l_j(ID_i) + \sum_{j=1}^{t} \Delta_j \pmod q$$

1.6. "Leave" Operation

Operation "Leave" is used when a node leaves a region. Any node j removes node i from its CRL when receiving Leave request from node i or detecting the node leaves.

1.7. "Merge" Operation

Operation "Merge" is used when the number of nodes in a region is under the threshold. It simply divides the region into many parts and they join to the other region respectively. It is shown in **Fig. 1**.

1.8. "Partition" Operation

Operation "Partition" is used when RTC of a region is under the GTC. **Figure 2** shows that AKM partitions share Si into Si and S(m+1). It first selects t regions from S1 to Sm and chooses t nodes {Sj, 1…Sj, t} from each Si region. Second, it creates a new node S(m+1) and joins into AKM. Furthermore, it partitions 2n nodes from Si into two nodes, Si and S(m+1):

$$S_t = \sum_{j=1}^{t} S_j l_j(ID_{s_t}) \pmod q$$

Where: $l_j(ID_{st}) = \prod_{r=1, r\neq j}^{t} \frac{ID_{St} - ID_{sr}}{ID_{sj}} \frac{ID_{sr}}{ID_{sr}} \pmod{}$

By Lagrange interpolation and:

$$S_j = \sum_{v=1}^{t} S_{j,v} l_{j,v}(0) \pmod q$$

Where:

$$l_{j,v}(0) = \prod_{r=1, r\neq j}^{t} \frac{IDs_{j,r}}{IDS_j - IDS_r} \pmod q$$

Thus:

$$S_t = \sum_{j=1}^{t} \sum_{v=1}^{t} S_{j,v} l_{j,v}(0) l_j(ID_{s_t}) \pmod q$$

1.9. "Expansion" Operation

Operation "Expansion" is used when RTC of a region is under the GTC. But when the RTC is equal to GTC in all AKM regions, it has to perform expansion operation to extend the hierarchy. As in **Fig. 3**, AKM extends region Si from one level to two levels. It selects t nodes in region Si and executes Operation join to create a new node Si, (n+1). It then moves Si,1, …, Si, m to be Si,(n+1)'s children, Si,(n+1),1, …, Si, (n+1),m with shares Si,(n+1),j, $1 \leq j \leq m$, that:

$$S_{i,(n+1),j} = a(ID_{i,(n+1),j}) = \sum_{r=1}^{t} a_r x^r \pmod q$$

where, ar = rr | sr ($1 \leq r \leq t$), Si,(n+1) = stst-1…s1 and all rrs are the same used in region Si. Region Si,(n+1) continues (n, t)- threshold as in region Si

The six-region-based operations form YeHLL's secret sharing scheme on MANET of AKM handle key management. The scheme does need Trusted Authority (TA) to start up, neither any central authorities to compute and distribute shares.

1.10. Performance Analysis

Computation cost on the MANET environment is a very important issue. Certain mobile ad-hoc devices have restricted power and cannot support jobs requiring heavy computation cost. In this section, it gives scheme's evaluation of communication, computation cost and large mobile nodes with existing schemes. The existing method given by (Lin and Lee 2010) can handle large number of nodes in MANET. But there is no such improvement for reducing communication and computational cost. Computational cost of our proposed method is less when compared with existing method. Almost all operands in modified AKM reduce, resulting from each modified AKM share as 1/t faster than AKM. Furthermore, the computation cost of all operations can be reduced to 1/t.

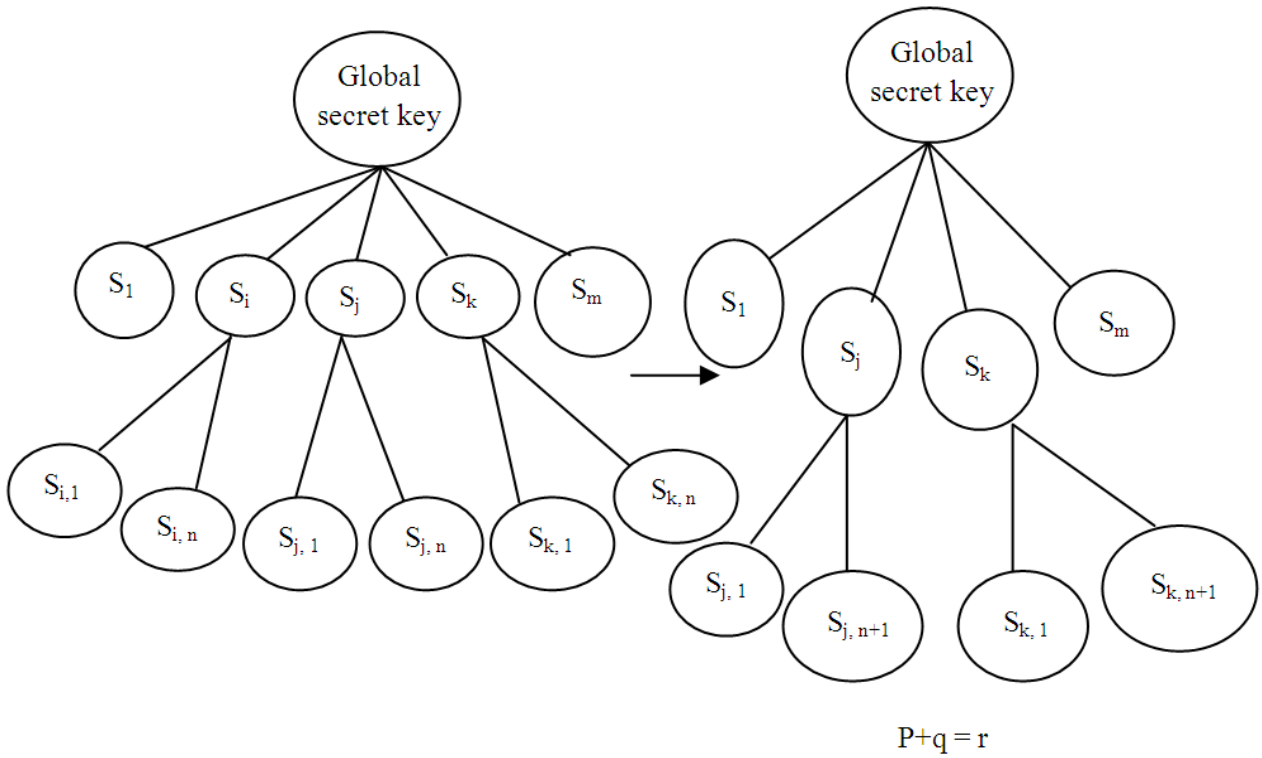

Fig. 1. Operation merge-merge S_i into S_j and S_k

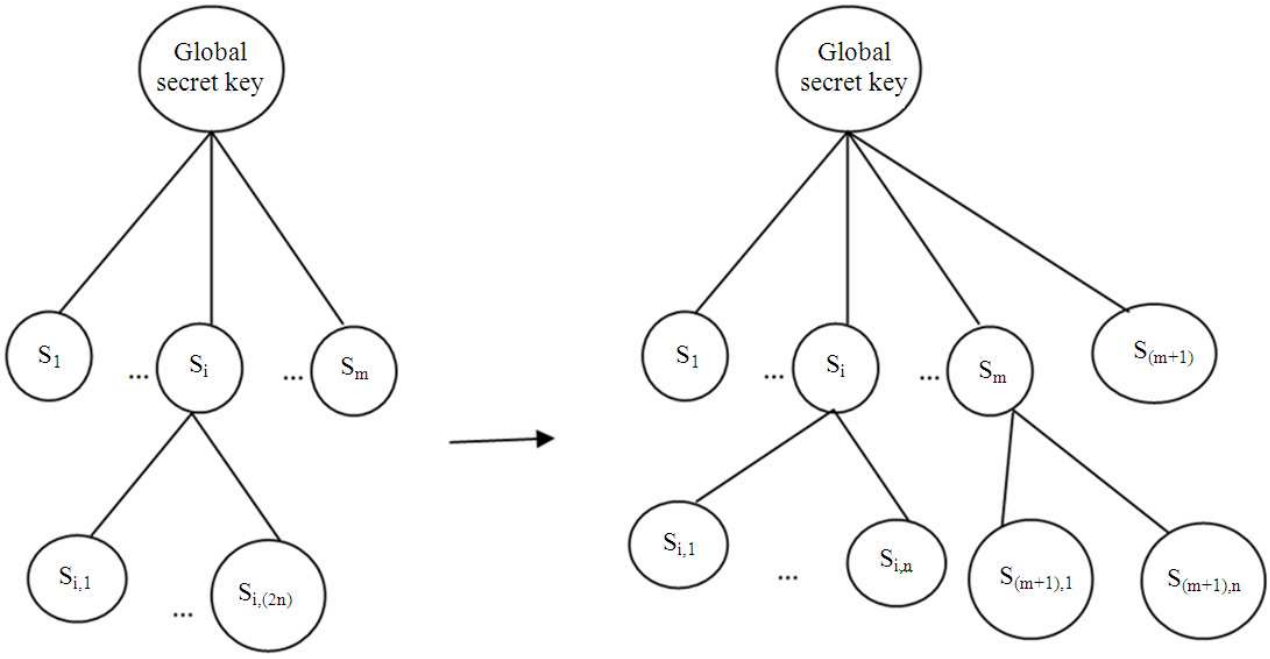

Fig. 2. Operation partition-partition Si into S_j and S(m+1)

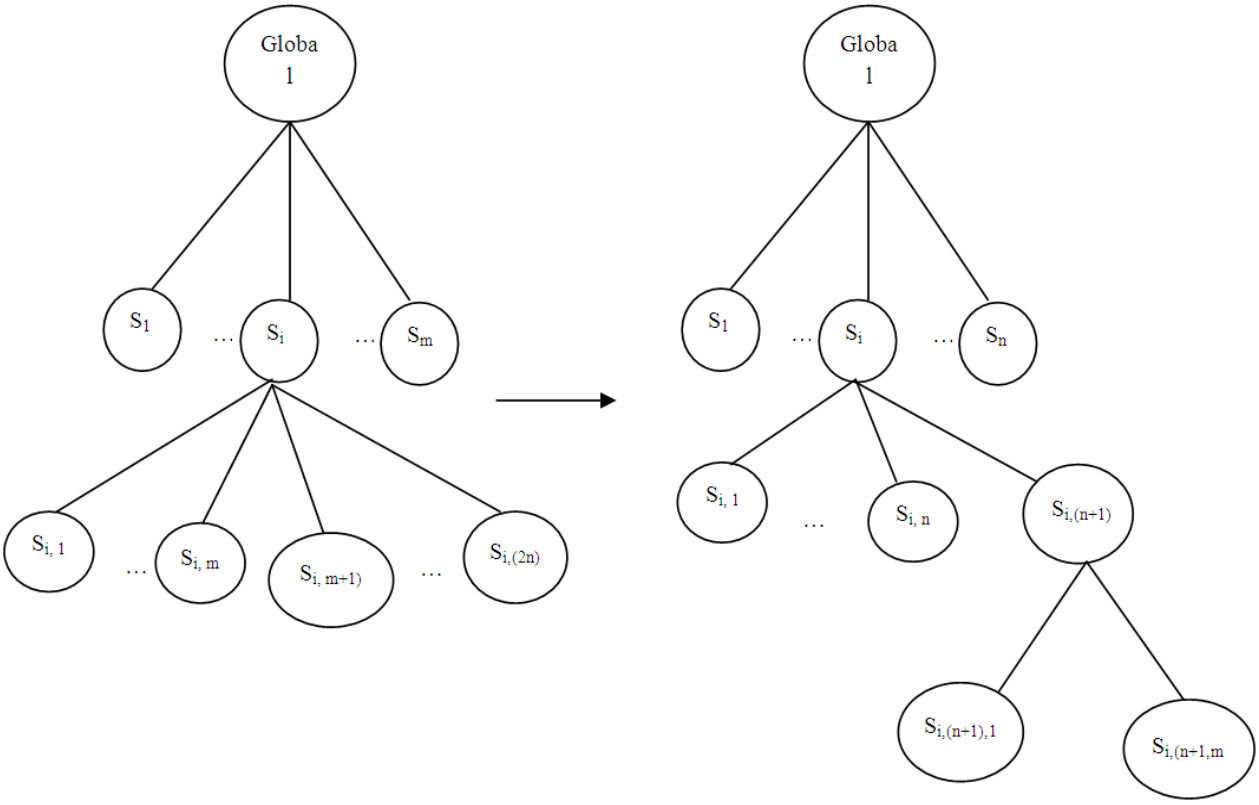

Fig. 3. Operation expansion

Proposed AKM inherits the AKM structure and transmissions between each node are (update) shares. Thus the single message discussion needs to be transmitted showing significant improvement. The length of secret key k, protected by the secret sharing scheme, must be long enough, such as 2048 bits or more for some security issues. In Shamir's secret sharing scheme, k is the constant in a(x) equation. The length of all the shares $a(x_i)=\sum_{j-1}^{t-1} a_j x^j + k, 1 \le i \le n$, is bounded by |k|.

For example, if |k| = 2048 bits long, the length of each share is at least 2048 bits. However, modified secret sharing scheme reduces share length to 1/t without security loss. The secret key is divided in each coefficient aj = rk | kj and k = k1,k2…,kt with the length |a(xi)| as 1/t of |k| on appropriate prime number p. This lets to reduce the computational cost.

1.11. Communication Cost

In addition, the overhead associated with the secret sharing communication may be seen as too costly for efficient operation. In such cases, it is possible to relax the security policy slightly to reduce the secret sharing overhead.

On the other hand, proposed scheme has a lower communication overhead. Comparsion between AKM and Proposed AKM for Message length comparsion is given in **Table 1**.

By considering the networks with 2000 nodes, the performance of the proposed approach is evaluated based on the communication overhead. The communication overhead of the existing scheme is 69%, where as the communication overhead of the proposed secured technique is very less (i.e., 48%) when compared to the existing technique and is shown in **Table 2**.

From **Fig. 4**, it is revealed that the communication cost of the proposed system of AKM technique has very low overhead when compared with approaches.

Thus Computational Cost, Communication cost is reduced along with large number of nodes.

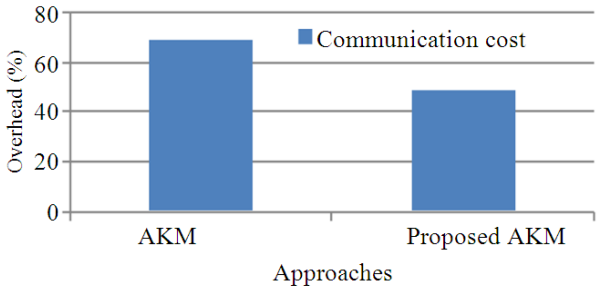

Fig. 4. Comparison of communication cost

Table 1. Message length comparison

Approaches	Length of message (share) size
AKM	$\|yi\| = \|k\| \leq \|p\|$
Proposed AKM	$\|y_i\| = \frac{\|k\|}{t} \leq \|k\| \leq \|p\|$

Table 2. Communication cost comparison

Approaches	Communication cost (%)
AKM	69
Proposed AKM	48

2. CONCLUSION

This study proposes the modified AKM to reduce the communication cost/computation cost to 1/t of the original cost without security loss. The scheme is security, efficient, independent of the infrastructure, tolerance to node compromise and easy to be deployment and also efficient for large number of nodes when compared with existing. From the comparison, the modified AKM is more practical because it can handle large number of dynamic nodes in MANET and provide sufficient security requirements.

3. REFERENCES

Blakley, G.R., 1997. Safeguarding cryptographic Keys. Proceedings of the AFIPS 1979 National Computer Conference, (CC' 97), Arlington, VA, pp: 313-317.

Francis, M., M. Sangeetha and A. Sabari, 2013. A survey of key management technique for secure and reliable data transmission in MANET. Int. J. Adv. Res. Comput. Sci. Soft. Eng., 3: 22-27.

Khdour, T. and A. Aref, 2012. A hybrid schema zone-based key management for manets. J. Theoritical Applied Inform. Tecnol., 35: 175-183.

Lin, C.H. and C.Y. Lee, 2010. Modified autonomous key management scheme with reduced communication/computation costs in MANET. Proceedigns of the International Conference on Complex, Intelligent and Software Intensive Systems, Feb. 15-18, IEEE Xplore Press, Krakow, pp: 818-821. DOI: 10.1109/CISIS.2010.70

Rafat, R.I. and M. Haque, 2009. Enhancing security for mobile ad hoc networksby usingelliptic curve cryptography. University of Dhaka.

Raghavendran, V., G.N. Satish and P.S. Varma, 2013. A study on contributory group key agreements for mobile ad hoc networks. Int. J. Comput. Netw. Inform. Security, 4: 48-56. DOI: 10.5815/ijcnis.2013.04.07

Shamir, A., 1979. How to share a secret. Commun. ACM, 22: 612-613. DOI: 10.1145/359168.359176

Wu, B., J. Wu and Y. Dong, 2008. An efficient group key management scheme for mobile ad hoc networks. Int. J. Security Netw.,4: 125-134. DOI: 10.1504/IJSN.2009.023431

Zhu, B., F. Bao and R.H. Deng, 2005. Efficient and robust key management for large mobile ad hoc networks. Int. J. Comput. Telecommun. Netw., 48: 657-682. DOI: 10.1016/j.comnet.2004.11.023