International Journal of Research in Engineering, Science and Management
Volume-3, Issue-7, July-2020
journals.resaim.com/ijresm | ISSN (Online): 2581-5792

Authenticated Group Key Agreement Protocol for MANET Based on Cryptographic Techniques

S. Noorjahan Asikka*
PG Scholar, Department of Computer Science and Engineering, Anna University College, BIT Campus, Thiruchirappali, India
*Corresponding author: ashikkahameed1357@gmail.com

***Abstract*: Mobile ad hoc networks (MANET) have been utilized in numerous application regions, for example, sensors, document sharing and vehicle-to-vehicle correspondences. Secured information correspondence is a basic issue for MANET. Bunching is a viable and down to earth approach to upgrade the security execution of MANETs. There are various issues identified with the utilization of bunch based gathering key understanding conventions in MANET, for example, adjustment in group based interchanges, safely choosing the group head for between bunch correspondences, giving secure gathering key update instrument for dynamic gatherings and diminishing expenses of interchanges and calculations. In this postulation, we propose a secure - effective transmission (SET) for cluster – based gathering key protocol (SGKP) that is versatile in MANET systems. We portray a novel secure bunch head determination component in the proposed convention. The convention gives security to dynamic gathering activities notwithstanding the fundamental security properties. The proposed convention additionally gives better execution as far as lessening the correspondences and computational expenses. The outcomes show that the proposed conventions have preferred execution over the current secure conventions for SGKPs, regarding throughput and vitality utilization.**

***Keywords*: MANET, Security, SET, SGKP, Cluster head selection and Throughput.**

1. Introduction

MANETs have been utilized in numerous application territories, for example, sensors, document sharing and vehicle-to-vehicle interchanges. Since substances in MANETs are versatile, giving secure interchanges among members are noteworthy issue. To conquer this issue, bunch key trade conventions are utilized. Such conventions are classified as key appropriation and key understanding conventions. In key appropriation conventions, there exists an incorporated position, for example, an element in the system or a confided in outsider, to circulate bunch keys to members. In key understanding conventions, all members in the gathering process a mutual key by utilizing some open parameters and capacities. Since MANETs are decentralized and portable systems, bunch key understanding conventions are preferable competitors over key conveyance conventions for giving secure interchanges.

2. Key Management in MANET Summary

MANET has some compels such its vitality compelled tasks, restricted physical security, variable limit connections and dynamic topology. In this way, there are diverse Key Management plans are utilized to accomplish the high security in utilizing and overseeing keys. The vital errand in MANET utilizes diverse cryptographic keys for encryption like symmetric and asymmetric key, group and hybrid key (for example blended of both symmetric and asymmetric key). Here we talk about a portion of the significant Key Management plots in MANET.

Symmetric Key: The same keys are used by source and destination. This key is used for encryption the data as well as for decryption the data. If n nodes needs to interconnect in MANET, k number of key pairs are required, where k=n(n-1)/2. Some of the symmetric key management schemes in MANET are Distributed Key–Pre Distribution Scheme (DKPS), Peer Intermediaries for Key Establishment (PIKE), and Key Infection (INF).

Asymmetric Key: It utilizes two-section key. Every beneficiary has a private key that is left well enough alone and an open key that is distributed for everybody. The sender turns upward or is sent the beneficiary's open key and uses it to scramble the message. The beneficiary uses the private key to unscramble the message and never distributes or transmits the private key to anybody. Therefore, the private key is never in travel and stays resistant. This framework is here and there alluded to as utilizing open keys. This decreases the danger of information misfortune and expands consistence the executives when the private keys are appropriately overseen. Some of the asymmetric key management schemes in MANET are Self-Organized Key Management (SOKM), Secure and Efficient Key Management (SEKM), Private ID based Key Asymmetric Key Management Scheme.

Group Key: It is a solitary key which is allotted just for one gathering of versatile hubs in MANET. For building up a gathering key, bunch key is making and circulating a mystery

for bunch individuals.

Secure choice of bunch heads is another noteworthy issue in MANETs. The general methodology in previous conventions is that every member freely reports the quantity of associations with different members. At that point, the one with the greatest number of association is chosen as a group head. Consequently, group head choice procedure is open for security dangers. For example, a noxious member can guarantee that it has the most elevated number of associations in its neighbourhood. At that point, the malignant member can control all the interchanges of the group.

3. Related Works

MANETs are framed by a mix of groups. Interchanges of members in MANET are ordered as in bunch and between group correspondences. The first is the correspondences of members that are the individual from a similar bunch. The subsequent one is the correspondences of members that are not the individual from a similar group. So as to compose secure correspondences for such bunch based system, the greater part of the current secure interchanges conventions utilize two level security draws near.

Sukin Kang [1], the key sharing among the gathering individuals is a significant issue for secure gathering correspondence in light of the fact that the correspondence for some, members suggests that the probability of illicit catching increments. The technique empowers the gathering individuals to just build up a gathering key and give high adaptability to dynamic gathering changes, for example, part join or leave and gathering combining or segment.

Lu, C.F [2], proposed a common confirmation and gathering key understanding convention for uneven remote systems. Tseng as of late proposed a novel secure convention to improve Bresson et al's. convention. Be that as it may, the two conventions depend on testament based open key frameworks and shaky against the supposed pantomime assaults. This paper proposes a certificate less validated gathering key understanding (cAGKA) convention dependent on elliptic bend discrete logarithms.

In [3], the current framework, the security gave at the information interface layer for huge Ethernet systems utilizing GKSP (Group based MAC key determination convention). Be that as it may, this plan has issues like security combination at organize layer, proficient key sharing and hub overhead and so forth.

Rather than performing individual rekeying activities [5], for example recomposing the gathering key after each join or leave demand, we examine a stretch based methodology of rekeying. We consider three stretches based circulated rekeying calculations, or span based calculations for short, for refreshing the gathering key: 1) the Rebuild calculation; 2) the Batch calculation; and 3) the Queue-cluster calculation. Execution of these three stretch based calculations under various settings, for example, extraordinary join and leave probabilities, is examined.

Min-Shiang [6], Based on the gathering Diffie–Hellman strategy, a contributory gathering key trade convention has been proposed by Biswas. In spite of the fact that Biswas asserted the convention has a place with a contributory gathering key trade. [7] Due to dynamic condition, there exist number of dangers as cell phones and hubs could openly move around in MANET, for example, spying of correspondences channels, Denial of Service (DoS), vulnerabilities of pantomime by malevolent insiders and so on.

Since it is conceivable to productively register one gathering key for all groups in MANET, bunch heads don't have to perform more tasks while sorting out between bunch interchanges.

4. Proposed System

In this paper, we propose the system model that contains a few bunches; each group has its facilitator in particular CH (initiator). The clusters are interconnected by means of CHs. There are subgroups of individuals called bunch in which one part is CH and virtual subgroup of CHs.

Our new key administration conspires to be specific "secure and effective transmission (SET) for group based gathering key protocol (SGKP)" Management plot that is a straightforward, effective and adaptable Group Key administration for MANETs. Numerous tree based multicast directing plan are utilized, which misuse way assorted variety for strength. In this way, in our plan, two multicast trees are utilized for every subgroup (for example group subgroups or CHs' subgroup). In MANET, fundamental main head in cluster MCH (its initiator) has the equivalent CH job, yet on the groups' subgroup. Our commitments in this investigation are recorded beneath:

- We propose a protected and productive transmission for bunch based gathering key convention for MANETs, to be specific SGKP by improving the security of convention in and by including another powerful gathering activity called the group blend activity.
- We propose a novel secure group head determination component for SGKP-MANET.
- SGKP gives protection from the known-key assaults characterized and better execution regarding lessening the interchanges cost and computational expense of registering and refreshing gathering key.
- Also gives proficient and secure gathering key calculation arrangement by taking out the security and execution issues in two-level gathering key understanding conventions for MANETs.
- A model application situation for SGKP on a hazardous situation correspondence with recreations is introduced.

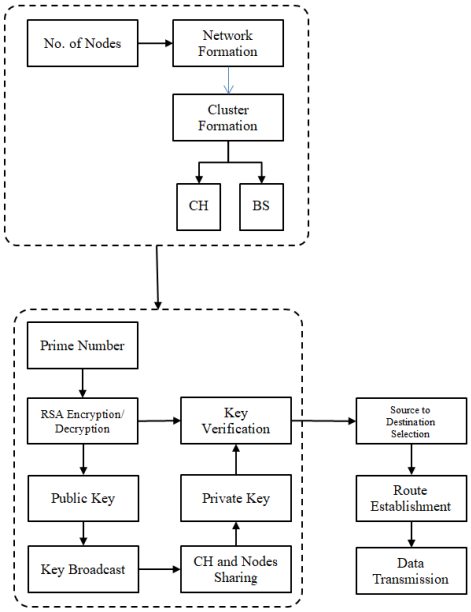

Fig. 1. System Architecture

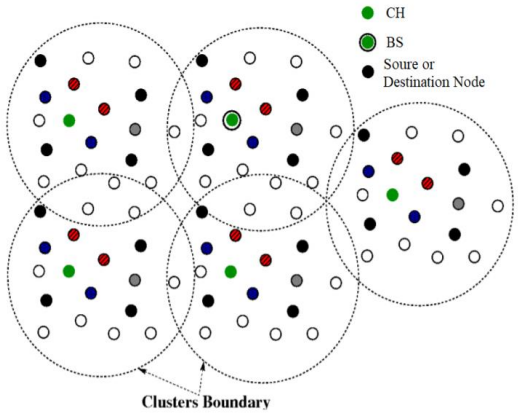

Fig. 2. Key Management in Cluster Based MANET

5. Secure and Efficient Transmission for SGKP

We proposed another methodology which intends to address the adaptability issue while thinking about the dynamic part of the gathering individuals and dynamicity of hubs in MANET. There are two trees on the system to maintain a strategic distance from the power issue too. Our methodology depends on bunching way. Each bunch is started by CH, to be specific group initiator or organizer initiator.

CH has then two keys; one for its bunch subgroup and another for the interconnection among the groups through CHs. Right off the bat, we depict our system model that is the versatile impromptu system dependent on bunching that contains for instance five groups as appeared in Fig. There is a CH for each bunch and one of CHs is MCH.

A. Interconnection among the Clusters

The interconnection among the clusters is by means of the MCH begins to introduce the procedure for a CHs' multicast subgroup by communicating a join publicizes message over the whole MANET. We guessed the hubs no change its shading, blue hub despite everything blue, red hub still red, dark hub despite everything dim and other CHs are source/recipient, by means of the CHs appears as a virtual bunch. So we can apply a similar situation that is utilized before in the bunch, to get blue and red multicast trees among all CHs in MANET.

B. Group Key Establishment Protocol

The possibility of subgroup key understanding convention is that all subgroup individuals keep up a rationale key's tree in nearby extra room. This current key's tree is utilized to reason the last normal subgroup key. Before presenting the security and execution properties of gathering key understanding conventions and the nitty gritty meaning of SGKP, we give the fundamental definitions identified with bunch hub, bunch head, open parameters and group ideas for the utilization of gathering key understanding conventions in MANETs. A SET plan actualized for SGKPs comprises of the accompanying tasks, explicitly, arrangement at the BS, key extraction and mark marking at the information sending hubs, and confirmation at the information getting hubs follows:

- *Setup:* The network BS (as a confidence specialist) generates a master key mk and public parameters for the private key generator (PKG), and gives them to all sensor nodes.
- *Extraction:* Given an ID string, a sensor node generates a private key sekID associated with the ID using mk.
- *Signature signing:* Given a message M, time stamp t and a signing key, the sending node generates a signature SIG.
- *Verification:* Given the ID, M, and SIG, the receiving node outputs “accept” if SIG is valid, and outputs “reject” otherwise.

The proposed SET-SGKP has a convention instatement preceding the system sending and we present the convention introduction; portray the key administration of the convention by utilizing the SET plan, and the convention activities a while later.

C. Protocol Initialization

In SET-SGKP, time is separated into progressive time stretches as other mean time stamps by Ts for BS-to-hub correspondence and by tj for leaf-to-CH correspondence. Note that key pre-dispersion is an effective strategy to improve correspondence security.

In this postulation, we embrace IDtk as client's open key under a SET plan, and propose a novel secure information transmission convention by utilizing SET explicitly for SGKPs. The relating private matching parameters are preloaded in the sensor hubs during the convention introduction. Along these lines, when a sensor hub needs to verify itself to another hub, it doesn't need to acquire its private key toward the start of another round. Upon hub repudiation, the BS communicates the undermined hub IDs to all sensor hubs; every hub at that point

stores the disavowed IDs inside the current round.

We embrace the additively RSA (Rivest–Shamir–Adleman) encryption plan to encode the irregular number of hub information, in which a particular activity performed on the plaintext is identical to the activity performed on the composite number. Utilizing this plan permits effective accumulation of scrambled information at the CHs and the BS, which additionally ensures information privacy. In the convention introduction, the BS plays out the accompanying tasks of key pre-dispersion to all the sensor hubs:

- Generate an encryption key k for the RSA encryption plan to encode information messages, where k = [m-1], m is a huge whole number.
- Generate the matching parameters and create stochastically. Pick two cryptographic prime capacities: H, for the point mapping hash work which maps strings to components, and h, for mapping subjective contributions to fixed-length yields.
- Pick an arbitrary number as the ace key mk, set P as system open key. Preload every sensor hub with the framework parameters.

Pseudo code: RSA

Key generation

1. Consider 6 large prime numbers p, q, r, s, t, and u.
2. Compute n=p*q*r*s*t*u.
3. Compute $\varphi(n)$= (p-1)*(q-1)*(r-1)*(s-1)*(t-1)*(u-1).Where$\varphi$is Euler's totient function. This value is kept private.
4. Choose an integer *e* such that *1 < e <φ (n) and gcd (e, φ (n)) = 1*; i.e., *e* and *φ (n)* are co-prime.
5. Find d, such that d*e mod $\varphi(n)$=1.

Publish e and n as the public key. (Or) public key= {e, n}

Keep d and m as the secret key. (Or) private key= {d, n}

Encryption

C= m^e(mod n)

Decryption

M= c^d(mod n)

6. System Implementation

In SGKP-MANET, first, every member in the gathering executes Cluster Head Selection Step to separate the gathering U into bunches. On the off chance that any noxious endeavour of a member is distinguished during the execution of this progression, the proprietor of the malignant endeavour is expelled from the gathering. When the groups are framed, every member in each bunch executes Temporary Public Key Distribution Step to process and circulate the transitory open keys to different members in its group. At that point, every member in the bunch executes Temporary Public Key Verification and Secret Key Distribution Step for confirming the approaching transitory open keys, processing and broadcasting its own mystery key to different members in its own group cluster.

Next, mystery keys are checked in Secret Key Verification Step. On the off chance that any malignant endeavour is distinguished either in brief opens key confirmation or in mystery key check, the proprietor of the pernicious endeavour is barred from the bunch key calculation. Each legit member in the bunch registers the group key. After the group keys are processed, Cluster Merge Step is executed to register a typical key for all bunches in the system. At last, Joining Non-Clustered Participants Step is executed if there exist any non-grouped members in the system. The subsequent key is indicated as a gathering key for a MANET. Also, Leaving Participants Step can be executed if any member leaves the gathering to refresh the gathering key. Subtleties of SGKP-MANET convention steps are as per the following:

A. Cluster Head Selection

Every hub and members arbitrarily chooses and communicates the RREQ-Route Request to the contiguous members in its system. Every member confirms the approaching communicate messages of each RREQ. At that point, every hub creates its own ACK RREP to the nearness network by checking approaching communicate messages.

After the confirmation, if no bamboozling member is distinguished, the member with the most extreme adjoining hub in its neighbourhood is chosen as the group head. If there should arise an occurrence of fairness, the member with the base ID is chosen as the group head. For example, let RREP the request are the members with the greatest adjoining hub in their neighbourhood. At that point, high worth hub is chosen as the group head.

B. Public Key Distribution and Verification

Every hub arbitrarily chooses two momentary mystery prime key, and its communicates to other member in the group. After the open keys are appropriated, every hub, where every hub indicates bunch number for some positive whole number l, checks the communicate messages for every hub.

After the communicate messages at RREQ and RREP are traded by hub in the bunch, every hub confirms the communicate messages for every hub in the group. Something else, hub set confirmation framework esteem isn't equivalent – it will "disappointment" and rehash.

C. RSA Cluster Key Computation

In the event that no malevolent (no disappointment) member is recognized, at that point computes the key private for every hub. After the bunch keys are determined, the information transmission activity is acknowledged to deliver an ace key for bigger gathering. Let be the bunches in MANET then the groups are prepared to transmit the information safely.

After the cluster information in transmission, the non-grouped members join the gathering. Then again, this progression is likewise utilized for including new members after the gathering key is figured. Let be the member set after the group confirmation step and the non-bunched hub can send information or act a transitional hub.

Table 1
Simulation parameters

Parameters	Values
Tool	NS2
No. of Nodes	40
Area	150 X 1500
Routing Protocol	AODV
Malicious Nodes	1, 2, 4
Traffic	CBR
Transport Layer	UDP
Mobility Type	Random Waypoint
Channel Type	Wireless Channel
MAC Type	IEEE 802.11
Antenna Type	Omni Directional Antenna
Queue Type	Drop Tail-Pri Queue
Queue Length	1000
Simulation START/STOP Time	0.0/5.0 s

7. Result and Discussion

To evaluate the security of the proposed protocols, we have to investigate the attack models in NS2 that threaten the proposed protocols and the cases when an adversary (attacker) exists in the network. Afterwards, we detail the solutions and countermeasures of the proposed protocols, against various adversaries and attacks.

On the other hand, SGKP-MANET follows exactly the same steps for cluster key computation. Therefore, the cluster key computation of SGKP-MANET provides security against the following attack models:

Impersonation Attack: The attack is defined as a variant of active attack model. In this model, an attacker tries to impersonate any participant in inter or outer cluster by producing fake temporary public key message and fake secret key message without knowing the long-term secret key.

Eavesdropping Attack: Eavesdropping attack is a passive attack model, which is used to obtain information by eavesdropping the communication messages among participants.

Replay Attack: Replay attacks are attack models that messages of any participant are repeated maliciously. For both communication rounds, participant messages contain timestamp M to prevent the system from replicated messages.

A. Performance metrics

On this paper, we now have used following efficiency metrics for evaluating effects of black hole assault and effectiveness of our detection algorithm:

1) Throughput (T)

It is the ratio of the whole number of bits transmitted (B_{tx}) to the time required for this transmission, i.e. the change of knowledge transmission finish time (have a tendency) (t_{end}) and start time (t_{start}). Unit of throughput is bps.

$$T = \frac{B_{tx}}{t_{end} - t_{start}}$$

2) End-End Delay

The tip-finish extend of an information packet is characterised as the information packet takes a point in time to travel from the supply node to the destination node. *D*is computed because the ratio of the sum of man or woman prolong of each and every acquired knowledge packet to the total quantity of data packets bought.

$$D = \frac{\sum_{i=1}^{N_{rec}} D_i}{N_{rec}}$$

3) Packet Delivery Ratio

The packet delivery ratio (PDR) of a receiver is characterized as the share of the number of data packets actually delivered over the number of knowledge packets transmitted by way of the source node.

$$PDR = \frac{no.\ of packetsrec.indest.}{no.\ of packetssendbysource}$$

In this paper, the performance of the proposed SGKP based security method is analyzed. Based on the analyzing results X-graphs are plotted. Throughput, delay, energy consumption are the basic parameters considered here and X-graphs are plotted for these parameters.

Finally, the results obtained from this module is compared with previous results and comparison X-graphs are plotted. Form the comparison result, final RESULT is concluded.

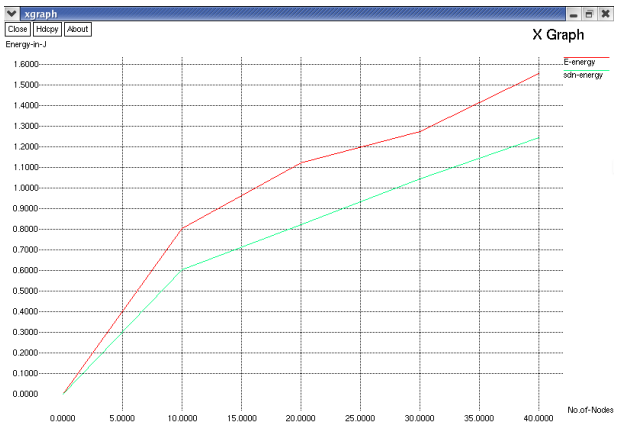

Fig. 3. Energy vs. No. of Nodes

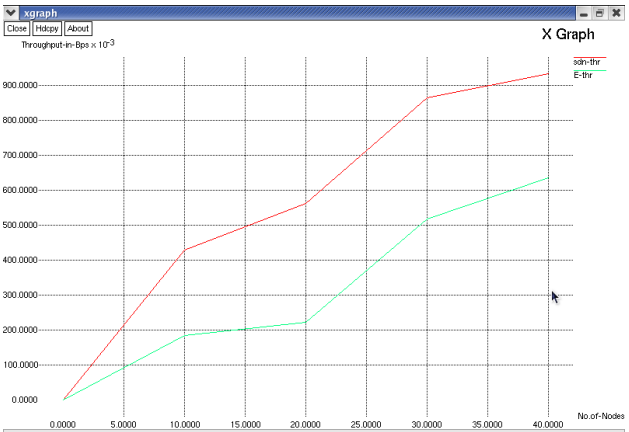

Fig. 4. Throughput vs. No. of Nodes

The figure 3 shows the utilization of energy in the SET proposed topology. The performance of proposed SET scheme with traditional distributed network control. This experiment considers the link failure issue for a single data flow, and the influence of other background traffic is not considered here. Due to the precise mobility detection in our scheme, the nodes can find the alternative paths in advance and avoid unnecessary traffic congestion due to link failure.

Figure 4 shows the response time for node mobility events, and is compared with the existing system with SGKP.

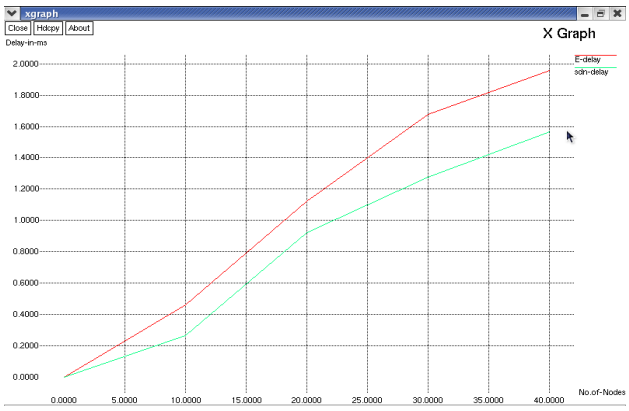

Fig. 5. Delay vs. Nodes

As shown in Figure 5, the proposed SET-SGKP scheme generates lower normalized routing overhead than the existing and proposed routing protocol. Finding new routes can introduce significant route discovery overhead due to node mobility in dynamic network topology. The goal of all these protocols include such as minimal control overhead, minimal processing overhead, multi-hop routing capability, dynamic topology maintenance, loop prevention, or more secure. Our paper focuses on the key management schemes that are important part of the security. As well, it has to be satisfied some features such as Security, Reliability, Scalability, and Robustness.

Security: intrusion tolerance means system security should not succumb to a single, or a few, compromised nodes. So, key management schemes should ensure no unauthorized node receives key material that can later be used to prove status of a legitimate member of the network.

Reliability: depends on key distribution, storage and maintenance and make sure that keys are properly distributed among nodes, safely stored where intruders aren't able to hack the keys and should be properly maintained.

Scalability: key management operations should finish in a timely manner despite a varying number of nodes and node densities. It makes use the occupied network bandwidth of network management traffic as low as possible to increase nodes' density.

Robustness: the key management system should survive despite Denial-of-Service attacks and unavailable nodes.

8. Conclusion

MANET is one of the most significant and remarkable applications. Because of the idea of temperamental remote medium information move is a significant issue in MANET and it needs security and unwavering quality of information. We at that point introduced secure and effective information transmission conventions, individually, for MANET arrange. Moreover, a novel and secure group head determination component has been proposed. Our examinations show that SET-SGKP has preferred execution results over the current ones regarding the correspondences and the computational expenses. For the computational cost examination, just the secluded exponentiation activities of key calculation steps have been thought of. To put it plainly, the presentation of SGKP is autonomous of the quantity of members in the gathering for the two interchanges cost and the computational expense. Reproduction results show that the proposed SET convention have preferable execution over existing secure conventions for SGKPs.

References

[1] Sukin Kang, CheongminJi, and Manpyo Hong. (2014), "Secure Collaborative Key Management for Dynamic Groups in Mobile Networks", Journal of Applied Mathematics, Vol. 2014, No. 601625.

[2] Lu, C.F., Wu, T.C., & Hsu, C.L. (2009). Certificate less Authenticated Group Key Agreement Protocol for Unbalanced Wireless Mobile Networks. WSEAS Transactions on Communications, 8 (11), 1145-1159.

[3] Digvijay Pawar. (2017), "Survey on Network Based Cryptographic Techniques for Key Generation and Data Encryption/Decryption", International Research Journal of Engineering and Technology, Vol. 04, No. 05, 1361-1363.

[4] B. Maheshwari. (2012), "Secure Key Agreement and Authentication Protocols", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.1, 113-126.

[5] Min-Shiang Hwang, Yung-Chen Chou, Chia-Chun Wu and Cheng-Ying Yang. (2018), "An Improvement of Tseng–Wu Group Key Exchange Protocol", Recent Developments in Intelligent Computing, Communication and Devices, Vol. 752, 693-698.

[6] Chan Yeob Yeuna, KyusukHanb, DucLiem Vob, Kwangjo Kimb. (2008), "Secure Authenticated Group Key Agreement Protocol in the MANET Environment", Information Security Technical Report, Vol. 13, No. 3, 158-164.

[7] Sriram TK, Yoga Vignesh B, Suji Helen L. (2017), "Group Key Agreement for Secured Group Communication", International Journal of Pure and Applied Mathematics, Vol. 117, No. 21, 1-9.

[8] He, D., Chan, S., & Guizani, M. (2017). Cyber security analysis and protection of wireless sensor networks for smart grid monitoring. IEEE Wireless Communications, 24(6), 98-103.

[9] Li, H., Lu, R., Zhou, L., Yang, B., & Shen, X. (2013). An efficient merkle-tree-based authentication scheme for smart grid. IEEE Systems Journal, 8(2), 655-663.

[10] Tseng, Y. M. (2007). A communication-efficient and fault-tolerant conference-key agreement protocol with forward secrecy. Journal of Systems and Software, 80(7), 1091-1101.

[11] Li, H., Lu, R., Zhou, L., Yang, B., & Shen, X. (2013). An efficient merkle-tree-based authentication scheme for smart grid. IEEE Systems Journal, 8(2), 655-663.

[12] Tseng, Y. M. (2007). A communication-efficient and fault-tolerant conference-key agreement protocol with forward secrecy. Journal of Systems and Software, 80(7), 1091-1101.

[13] Balaji, S., Julie, E. G., Robinson, Y. H., Kumar, R., & Thong, P. H. (2019). Design of a security-aware routing scheme in Mobile Ad-hoc Network using repeated game model. Computer Standards & Interfaces, 66, 103358.

[14] Ermiş, O., Bahtityar, Ş., Anarim, E., & Çağlayan, M. U. (2015). An improved conference-key agreement protocol for dynamic groups with efficient fault correction. Security and Communication Networks, 8(7), 1347-1359.
[15] Altop, D. K., Seymen, B., & Levi, A. (2019). SKA-PS: Secure key agreement protocol using physiological signals. Ad Hoc Networks, 83, 111-124.
[16] Liu, T., Gu, T., Jin, N., & Zhu, Y. (2017). A mixed transmission strategy to achieve energy balancing in wireless sensor networks. IEEE Transactions on Wireless Communications, 16(4), 2111-2122.
[17] Tan, C. H., & Teo, J. C. M. (2006, April). Energy-efficient ID-based group key agreement protocols for wireless networks. In Proceedings 20th IEEE International Parallel & Distributed Processing Symposium (pp. 8-pp). IEEE.
[18] Zhao, S., Aggarwal, A., Frost, R., & Bai, X. (2011). A survey of applications of identity-based cryptography in mobile ad-hoc networks. IEEE Communications surveys & tutorials, 14(2), 380-400.
[19] Hwang, M. S., Chou, Y. C., Wu, C. C., & Yang, C. Y. (2019). An Improvement of Tseng–Wu Group Key Exchange Protocol. In Recent Developments in Intelligent Computing, Communication and Devices (pp. 693-698). Springer, Singapore.
[20] Zhu, H., Zhang, Y., & Zhang, Y. (2016). A Provably Password Authenticated Key Exchange Scheme Based on Chaotic Maps in Different Realm. IJ Network Security, 18(4), 688-698.