ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Hybrid Key Aggregation Model for Privacy Preserving Group Key Protocol

Garubilli Jyothi
M.Tech Student,
Dept of CSE,
Pydah College of Engineering and Technology, Gambheeram, Visakhapatnam.

Meduri Kamalakar
Associate Professor,
Dept of CSE,
Pydah College of Engineering and Technology, Gambheeram, Visakhapatnam.

Dr. Ramesh Challagundla
Professor,
Principal,
Pydah College of Engineering and Technology, Gambheeram, Visakhapatnam.

Abstract:
Key aggregation or group key protocol mechanism over multiple or group users is always an interesting research issue in the field of secure group key generation. Simple symmetric and asymmetric approach may not give the optimal results, so it is a polynomial approach where aggregated key can be generated from multiple users and distributed asynchronously. Here the key can be computed from part of the shared keys from all the users and data can be encoded with a novel cryptographic approach which uses grid transpose technique. Our experimental results show more accurate results than traditional approaches

Introduction:
Wireless sensor networks are the networks to monitor physical or environmental situations. The modern networks are bi-directional and also enabling the control of sensor activity. The improvement of wireless sensor networks was spurred by military applications, for example, war zone observation; today such networks are utilized as a part of numerous modern and buyer applications, for example, mechanical process checking and control, machine wellbeing checking the criteria[1][2]. Be that as it may, sensor gadgets are helpless against noxious assaults, for example, pantomime, block attempt, catch or physical demolition, due to their unattended agent Situations and breaches of availability in wireless correspondence. Along these lines, security is one of the most vital issues in numerous basic element WSN applications. Dynamic WSNs along these lines need to address key security prerequisites, for example, hub validation, information classification furthermore, trustworthiness, at whatever point and wherever the nodes move[3]. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hopwireless mesh network[4][5]. Symmetric key plans are not reasonable for versatile sensor hubs and along these lines past methodologies have concentrated just on static WSNs. A couple approaches have been proposed in view of PKC to bolster dynamic WSNs. Hence, in this area, we audit past PKC-based key administration plans for element WSNs and break down their security shortcomings or disservices.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Related Work:

A sensor hub can't specifically build up a pairwise key with other sensor hubs and, it requires the support of the group head. In their plan, in request to set up a pairwise key between two hubs in the same bunch, the group head haphazardly creates a pairwise key and encodes it utilizing the mutual keys with these two hubs. At that point the bunch head transmits the encoded pairwise key to every hub. Therefore, if the bunch head is traded off, the pairwise keys between non-traded off sensor hubs in a similar bunch will likewise be traded off[6][7]. Moreover, in their scheme, in order to share a pairwise key between two nodes in different clusters, these two nodes must communicate via their respective cluster heads. So, after one cluster head generates the pairwise key for two nodes, the cluster head must securely transmit this key to both its node and the other cluster head. Thus, this pairwise key should be encrypted by using the shared pairwise key with the other cluster head and the shared key with its node, respectively. In this manner, if the pairwise key between the cluster heads is uncovered, all pairwise keys of the two hubs in various clusters are uncovered. The plan by bolsters forward and in reverse mystery by utilizing a key upgrade handle at whatever point another hub joins the cluster on the other hand if a hub is traded off. In any case, the plan does not give a procedure to ensure against clone and pantomime assault[8]. ID-PKC based key management schemes supporting the mobility of nodes in dynamic WSNs which removes the certificate management overhead. However, their schemes require expensive pairing operations. Although many approaches that enable pairing operations for sensor nodes have been proposed, the computational cost required for pairing is still considerably higher than standard operations such as ECC point multiplication[9][10].

Proposed system:

In this paper we propose an efficient key aggregate mechanism for secure key generation between multiple users.

It can be constructed from shared key pairs from the individual users, key can be easily distributed to the new users even though they are not directly communicates with other group people and encoding mechanism maintain data confidentiality with grid transpose mechanism without forwarding the data component directly. This proposed approach is simple and stronger in performance and security factors because key need not to be forwarded directly to any one and data cannot be transmitted directly or simply in terms of cipher blocks. We are proposing geo code based approach for identification of the nodes and authentication can be verified by key distribution centre with verification shares, secure session based group key can be generated for every transmission. Our work identifies the malicious nodes, authenticate the genuine users, encode and decode the data transmitted between source node to destination and it can be decrypted only at destination node even though transmission done through intermediate nodes.

Recurive and dynamic Key Generation:

There are some notations such as ‘n’ is number of members in the group. ‘x’ is public key for user. ‘N’ is large prime number.

(1) The first member computes T_1 (x) and sends it to the second member.

(2) The second member computes T_2 (x) and sends it to the third one.

(3) Repeat this until the last member computes $T_{rn}(x)$ and sends it to the first member.

(1) The first member computes Tr1 (Trn(x)) and sends it to

the second member.

(2) The second member computes T_2 (T_1 (x)) and sends it to the next.

(3) Repeat this until the last member computes $T_{rn}(T_{rn-1}$ (x)) and sends it to the first member.

Stage i.

(1) The first member computes T_1 ($T_{rn}(\cdot \cdot \cdot T_{rn-i+2}(x))$) and sends it to the second member.

(2) The second member computes Tr2 (Tr1 ($\cdot \cdot \cdot Tr_{n-i+3}(x)$))

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

and sends it to the next.
(3) Repeat this until the last member computes $T_{rn}(T_{rn-1}(\cdots T_{rn-i+1}(x)))$ and sends it to the first member.
By n − 1 stages message exchange by any member and the
ith member computes the group session key by:
$T_i\ (T_{i-1}\ (\cdots T_1(T_n(T_{n-1}(\cdots T_{i+1}(x))))))$ which is equal to
$T_{12....rn}(x)$

Cryptographic implementation:

Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA) block cipher. It is so named because it applies the Data Encryption Standard (DES) cipher algorithm three times to

The standards define three keying options:

- Keying option 1: All three keys are independent.
- Keying option 2: K1 and K2 are independent, and K3 = K1.
- Keying option 3: All three keys are identical, i.e. K1 = K2 = K3.

Keying option 1 is the strongest, with 3 x 56 = 168 independent key bits.

Keying option 2 provides less security, with 2 x 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K1 and K2, because it protects against meet-in-the-middle attacks.

Keying option 3 is no better than DES, with only 56 key bits. This option provides backward compatibility with DES, because the first and second DES operations simply cancel out. It is no longer recommended by the National Institute of Standards and Technology (NIST) and not supported by ISO/IEC 18033-3.

Conclusion and Future Work:

We have been concluding our current research work with segmented nodes, efficient authentication with signatures and dynamic key exchange protocol for secure and dynamic key generation.

Key can be generated dynamically during the eviction and member addition. We can improve our current research work with density based clustering model because nodes need not to be clustered with only latitude and longitudes of the nodes, we can integrate the various parameters like signal strength, channel capacity etc… when we have more number of nodes in the zone. We can improve the data confidentiality by creation of complex key instead of simple delta value with same cryptographic model.

References:

[1]. Kamanashis Biswas and Md. Ali, “Security threats in Mobile ad hoc networks”, University essay from Blekinge Teknisha Ho gskola/Sektionen for Teknik (TEK), 2007.

[2] M Poturalski, P. Papadimitratos, J. Hubaux, “Secure Neighbor Discovery in Wireless Networks,” In Proceedings of the 2008 ACM symposium on Information, computer and communications security, Tokyo, Japan, 2008.

[3] Jameela Al-Jaroodi, “Security Issues In Wireless Mobile Ad Hoc Networks (MANET)”, Technical Report TR02-10-07, University of Nebraska-Lincoln, 2002.

[4] William Stallings, “Cryptography and Network Security: Principles And Practices”, 3rd Edition, Prentice Hall 2003, ISBN: 0-13-091429-0.

[5] Klas Fokine, Key Management in Ad Hoc Networks, Master Thesis, Linkping University, 2002. http://www.liu.se/.

[6] ITU-T Recommendation X.509, ―Public-key and attribute certificate frameworks‖, August 2005.

[7] C. Siva Ram Murthy and B.S. Manoj, ―Ad Hoc Wireless Networks: Architectures‖, book, ISBN 0-13-147046-X, first printing, 2004.

8] Xing Fei; Wang Wenye, ―Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks‖, MILCOM 2006, Oct. 2006, pp. 1 – 7.

[9] Bo Sun, Kui Wu, Yang Xiao, and Ruhai Wang, ―Integration of Mobility and Intrusion detection for wireless ad hoc networks‖, International Journal of Communication Systems, pp. 695 – 721, 2007.

[10] Y. Zhang, W. Lee, and Y. Huang, ―Intrusion Detection Techniques for Mobile Wireless Networks‖, ACM Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

BIOGRAPHIES:

Garubilli Jyothi, Currently pursuing M.Tech (Computer Science and Engineering), Pydah College of Engineering and Technology, Gambheeram, Visakhapatnam. Her research interests are Networks, Network Security and data mining.

Meduri Kamalakar, is currently working as an Associate Professor,in Computer Science and Engineering at Pydah College of Engineering and Technology, Gambheeram, Visakhapatnam. He has more than 10 years of teaching experience in field of computer science. His research interest includes Information Security and Networks.

Dr.Ramesh Challagundla, M.E, PH.D, MIEEE (USA), FIETE (IND), MIE (IND), MISTE is a former faculty of Birla Institute of Technology, Gitam University, ANITS and currently working as Professor and Principal of Pydah College of Engineering and Technology, Visakhapatnam.