

Secure Transmission To Remote Cooperative Groups With Minimized Communication Overhead

K.Udaya Ravi Kiran

Student, Department of Computer Science
UCEK, Kakinada
Andhra Pradesh, India
uday.kr@gmail.com

Mrs.Usha Devi SSSN

Assistant Professor, Department of Computer Science
UCEK, Kakinada
Andhra Pradesh, India
usha.jntuk@gmail.com

Abstract— In Wireless Mesh networks there is a need to Multicast to a remote cooperative group using encrypted transmission. The existing paradigms failed to provide better efficiency and security in these kind of transmissions. A major challenge in devising such a system involves in achieving efficient usage of Bandwidth and Reducing the number of unintended receivers. In this paper we circumvent these obstacles and close this gap by involving a sender based algorithm .This new paradigm is a hybrid of traditional Multicasting, shortest path techniques and group key management. In such a system, for every source destination pair the protocol adaptively calculates the mean delays along all the utilized paths and avoid the paths with greater or equal mean delays. Which eventually reduces the usage of unwanted paths and also results in reducing the number of unintended receivers at a considerable rate. This approach efficiently deals with the computation overhead and usage of network resources. Further more our scheme provides better security by reducing the number of unintended receivers..

Keywords- *Wireless Mesh Networks, Group Key Management, Multicasting, Remote Cooperative Groups.*

I. INTRODUCTION

Wireless Mesh Networks are suggested as the promising low cost approach to provide high bandwidth networks to the last mile.

A. *Wireless Mesh Networks*

A wireless mesh network is a communication network spread out among number of nodes organized in mesh topology. These nodes are Radio transmitters that are able to function as a wireless router. The mesh clients are Laptops, Mobile Phones and Many Other Wireless devices. The Mesh Routers forwards the Traffic From and To Gateways. These Networks are reliable and offer redundancy. As these nodes are connected in Mesh Topology, when one node in the network failed the other nodes are still able to communicate with each other either directly or indirectly through one or more intermediate nodes. These are also called self form and self heal networks. They can be implemented using the Common wifi Standards 802.11a,b,g or combinations of more than one of those standards.

WMN's infrastructure is a network of routers without any wired connections in between the nodes. It's Build of Radio Devices which can be connected wirelessly and they don't need any tradition access points like WLAN. This infrastructure is especially useful in carrying data over large distances. The infrastructure splits the distances into a series of short hops. This helps in boosting of signal by intermediate nodes. The intermediate nodes cooperatively pass data from Node 1 to node 2 by making decisions depending on the knowledge they have on the network. These kind of architectures provide high bandwidth, efficiency over a large coverage area.

Wireless Mesh Network's Operation principle is similar to the way how the packets travel across wired Internet. Each time the packet reaches another Node, a hop occurs. The data

hops from one device to another device until it reaches the destination. This is happend with the implementation of dynamic routing algorithms by each device. To Implement such routing protocols each device needs to communicate with other devices in the network over the routing information. Then depending on the protocols, the devices are able to determine what they can do with the data they receive, either to pass it to the next device or to keep it. The routing algorithms used should ensure that the data is transmitted through the most appropriate route on it's way to destination.

II. RELATED WORK

Key Management is the major security Concern in group oriented Communications. The existing key management systems can be categorised in to 2 types depending n the approaches. They are Group Key Agreement and Key Distribution systems. Presently both of these are active research areas and they have a huge repositories of literature.

A. *Group Key Agreement*

In Group key Agreement a group users are allowed to Negotiate over a Common Secret key. Then any member of the group can be able to encrypt a confidential message with this shared secret key so that only the group members are able to decrypt that message. This is one way to establish a secured intragroup broadcast channel without depending on a fully trusted key generation center to generate and distribute keys among the potential members of the group. A large number of group key agreement protocols have been proposed [1]-[8]. The earlier effort [1][2] focused on secure and efficient key distribution and group key management. Later studies [3] worked on efficient member joins, but effective work over member leaves is highly needed. Then the key establishment using one way function trees, and tree key structures [4][5][6] improved the efficiency for member joins and leaves. The Analysis in [9] proved that for the Lower bound for multicast

key distribution the lower bound worst case cost for a member join or leave is $O(\log n)$ rounds of interaction, Where the Number of group members is denoted by 'n'. Optimizing the rekeying cost in group key agreement schemes is achieved in [7]. The ring based structure proposed in [8] breaks the traditional round based interactions barrier, because in ring based structure a constant number of rounds are required for member addition and deletion.

B. Key Distribution System

In key distribution system, a fully trusted and centralized key server is present which allocates the secret keys to all potential users, such that only the potential users are able to read the transmitted messages. In the earlier key distribution protocols [10] the member addition or deletion is not supported after the system is deployed. Which was evolved in later works allowing the sender to choose the intended receivers in the initial group, referred to as Broadcast encryption.

From the literature broadcast encryption scheme is classified into two categories. Symmetric key Broadcast encryption scheme and Public key Broadcast encryption scheme. In symmetric key Broadcasting, The trusted center only generates all the secret keys and transmits messages to all the users, hence only the trusted center can be the sender.

In Public key broadcasting, the trusted key generation center generates a public key for all users along with the secret keys for each users. so that anyone can be the sender or broadcaster. Broadcast encryption in Symmetric setting was first formalized by fiat and Naor [11]. Naor and Pinkas [12] presented the first public key broadcast encryption for public encryption setting. The scheme will become insecure If users more than this threshold is revoked, hence it is not fully collusion resistant. the recent works in [13] presented a fully collusion resistant public key encryption scheme that has $O(\sqrt{N})$ complexity for key and cipher text sizes and for computation cost. The maximum allowable number of potential receivers is denoted by N. The more recent scheme [14] reduced the size of key and cipher texts, although it follows the same complexity as [13]. In [15] An upto date scheme was presented to improve the security concept of Public key broadcast encryption schemes, while keeping the complexity $O(\sqrt{N})$ same as in [13]. The Upto date work in [17] introduced the session key concept to provide additional security.

III. EXISTING SYSTEM

Fast transmission to remote cooperative groups establishes a secure connection between the user and the remote group. It's contribution includes two aspects.

A. Existing System Contributions

1) Secure Transmission

First it formalized the problem of secure transmission to a remote group, in which the core concept is to establish a secure and efficient one-to-many channel.

The recent efforts proposed by the authors [16] at eurocrypt 2009 provided solution for secure communtion from a remote sender to a remote cooperative group.

The authors proposed Asymmetric Group key agreement, in which the members of the group first negotiate over a common

public key, and each hold a different secret key. Then any sender who knows the public key of the group can securely transmit the message to group members by encrypting the message using the group key. Only the members of the group are able to decrypt the message.

2) New Key Management Paradigm

It proposed a new key management paradigm which is a hybrid of public key broadcast encryption and group key agreement. In this each member of the group has a public/Secret key pair. By knowing the public keys of the members of the group the remote sender can securely broadcast the secret session key to any intended subgroup chosen in adhoc way. Simultaneously, using this session key any message can be encrypted to the intended receivers. Only the selected Subgroup (members of the group) can jointly decrypt the session key and hence the Encrypted message. And in this approach the need of a fully trusted key server is eliminated

B. System Model

Consider the group is composed on N users, (U_1, U_2, \dots, U_N). The Sender wanted to send message to a Subset S of N users, where the size of the Subset S is $n \leq N$. Each Receiver in the group obtains a public/secret key pair by running keyGeneration algorithm (algorithm 1). The Public key is certified by CA (Certificate Authority). The secret key is kept only by the receiver, which is not shared with anyone. The Remote sender retrieves the public keys from the CA and validates their authenticity by checking its certificates. This results in no direct contact between the remote sender and the receivers. Now the sender can send encrypted messages to any chosen subset of receivers.

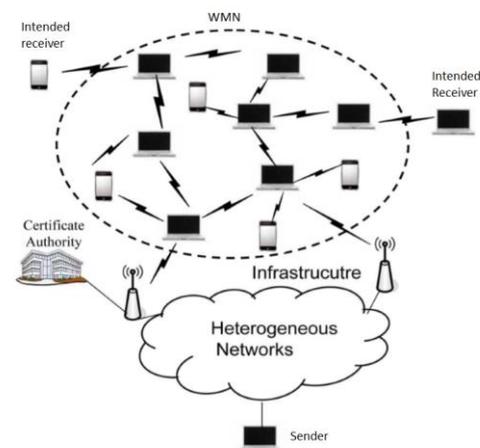


Figure 1. Architecture of Existing System

First the remote sender runs the Encryption algorithm (algorithm 2) to securely transmits the session key to the intended receivers of the group by choosing them in adhoc way. Then Members of the group who received this session key jointly can decrypt the message to obtain the session key using DecryptionAlgorithm(algorithm-3). Only those members who received this session key can only participate in further message transmission. Because all the further messages that are transmitted are encrypted using the session key.

C. Polynomial Algorithms Mentioned Above:

1) Algorithm 1:

KeyGen(i, n, N): This Key generation algorithm is run by each member of the group $U_i \in (U_1, U_2, \dots, U_N)$ to generate their own public / secret key pair. The user takes system parameters n, N and his index $i \in (1, 2, \dots, N)$ as inputs. The algorithm generates outputs $\langle pk_i, sk_i \rangle$ as his public / secret key pair.

2) *Algorithm 2:*

Encryption($S, \langle pk_i \rangle_S$): This algorithm is run by the sender who may or may not be one among the N members of the group. We assume that the sender already knows the public keys of the intended receivers. The sender gives the input as recipient set S and the public key pk_i for $U_i \in S$. The algorithm generates output pair $\langle Hdr, k \rangle$, where Hdr is the Header and k is the message encryption key (session key). (S, Hdr) is sent to the Receivers.

3) *Algorithm 3:*

Decryption ($U_j (sk_j) S, Hdr, \langle pk_i \rangle_S$): This algorithm is run jointly by the members of the intended receivers group to extract the secret key k hidden in the Header (Hdr). Header (Hdr) and Public keys of the receivers in the recipient set S are the common inputs. Along with those each receiver U_j privately inputs his secret key sk_j . This Outputs the same session key k for each user in S .

Encryption, Decryption algorithms are further represented in the latest works [17].

IV. PROPOSED SYSTEM

In the proposed system a routing algorithm is integrated, with the concept of fast transmission to remote cooperative groups, to improve the efficiency and security. This proposed system is a hybrid of multicasting, shortest path technique, and group key management. In this, for every pair of source and destination nodes, the protocol calculates the mean delays along all the available paths between the source and destination, and chooses the path with least mean delay. The core concept of this proposed system is to increase the security by reducing the number of unintended receivers, efficient usage of network resources. The disadvantage of the existing system is its broadcasting technique, in which not only intended receivers but all the members of the group will receive the message. But in the proposed system with the integration of routing algorithm we reduce the number of unintended receivers using the routing and multicasting techniques. The protocol calculates the shortest path to the destination nodes and uses it. The transmission follows multicasting as there can be more than one intended receiver. This technique remarkably reduces the number of unintended receivers and reduces the wastage of bandwidth and other network resources at a considerable amount.

A. Routing Algorithm

Link State Routing: This algorithm is embedded in each and every node, router in the network.

The link State Routing algorithm works in 5 stages.

- Each node Discovers all its neighbours.
- Measures the delay or cost to each of its neighbours.
- Constructs a packet telling all it has learned.
- Sends this packet to all other routers in the network.
- Computes the Shortest Path To every other router in the network.

First each router discovers all its neighbours. Then they measure the delay or cost of the path to each of its neighbours by reasonable estimate delay. This can be achieved by sending an echo packet to neighbour and ACK (acknowledgement) is needed. When the ACK packet is received the total time taken for the packet since it's sent to till it is received is considered as trip time and is divided into half which gives the avg or approximate time/cost to that neighbour. Then the Router constructs a packet including all this information which includes the delay or cost of the paths to all its neighbours from it will be included in that packet. This information packet is sent to all the other routers in the network by using flooding concept.

To keep the flooding in check, each packet contains source sender name, a sequence number which is incremented each time it is sent to another router. When the Destination name and the source sender name is same the packet will be discarded. When a router receives two packets from different senders at same time then the packet with highest sequence number is accepted assuming it is the most recent packet which might contain latest information. Then every router, uses all the received information packets along with its own information packet to construct a table which is used to compute the shortest path to every other node.

B. Advantages

- Reduces the wastage of bandwidth and other network resources.
- Improves security by reducing the number of unintended receivers at a considerable rate.

V. CONCLUSION

In this paper a Routing based technique for fast transmission to remote cooperative groups is proposed to achieve efficient usage of bandwidth and network resources. The proposed concept improves the security and focuses on calculating and choosing the shortest path between source and destination. It can reduce the number of unintended receivers and wastage of bandwidth, network resources.

REFERENCES

- [1] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," *Adv. Cryptol.*, vol. 950, EUROCRYPT'94, LNCS, pp. 275–286, 1995.
- [2] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, "The versa key framework: Versatile group key management," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 9, pp. 1614–1631, Sep. 1999.
- [3] M. Steiner, G. Tsudik, and M. Waidner, "Key agreement in dynamic peer groups," *IEEE Trans. Parallel Distrib. Syst.*, vol. 11, no. 8, pp. 769–780, Aug. 2000.
- [4] A. Sherman and D. McGrew, "Key establishment in large dynamic groups using one-way function trees," *IEEE Trans. Softw. Eng.*, vol. 29, no. 5, pp. 444–458, May 2003.
- [5] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement," *Trans. Inf. Syst. Security*, vol. 7, no. 1, pp. 60–96, Feb. 2004.
- [6] Y. Mao, Y. Sun, M. Wu, and K. J. R. Liu, "JET: Dynamic join-exit tree amortization and scheduling for contributory key management," *IEEE/ACM Trans. Netw.*, vol. 14, no. 5, pp. 1128–1140, Oct. 2006.
- [7] W. Yu, Y. Sun, and K. J. R. Liu, "Optimizing the rekeying cost for contributory group key agreement schemes," *IEEE Trans. Depend. Secure Comput.*, vol. 4, no. 3, pp. 228–242, Jul.–Sep. 2007.
- [8] R. Dutta and R. Barua, "Provably secure constant round contributory group key agreement in dynamic setting," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 2007–2025, May 2008.

- [9] J. Snoeyink, S. Suri, and G. Varghese, "A lower bound for multicast key distribution," Proc. IEEE INFOCOM, pp. 422–431, 2001
- [10] I. Ingemarsson, D. T. Tang, and C. K. Wong, "A conference on key distribution system," IEEE Trans. Inf. Theory, vol. 28, no. 5, pp. 714–720, Sep. 1982
- [11] A. Fiat and M. Naor, "Broadcast encryption," Adv. Cryptol., vol. 773, CRYPTO'93, LNCS, pp. 480–491, 1993.
- [12] M. Naor and B. Pinkas, "Efficient trace and revoke schemes," in Proc. 4th FC, 2001, vol. 1962, pp. 1–20.
- [13] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," Adv. Cryptol., vol. 3621, CRYPTO'05, LNCS, pp. 258–275, 2005.
- [14] J.-H. Park, H.-J. Kim, M.-H. Sung, and D.-H. Lee, "Public key broadcast encryption schemes with shorter transmissions," IEEE Trans. Broadcast., vol. 54, no. 3, pp. 401–411, Sep. 2008.
- [15] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," Adv. Cryptol., vol. 5479, EUROCRYPT'09, LNCS, pp. 171–188, 2009.
- [16] Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer, "Asymmetric group key agreement," Adv. Cryptol., vol. 5479, EUROCRYPT'09, LNCS, pp. 153–170, 2009.
- [17] Qianhong Wu, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Jesus A. Manjón, "Fast Transmission to remote Cooperative groups: A new Key Management Paradigm", Networking, IEEE/ACM Transactions on (Volume:21, Issue:2), pp.621–633, April-2013.