SECURITY SERVICES IN GROUP COMMUNICATIONS OVER MOBILE AD HOC AND WIRELESS SENSOR NETWORKS

Aditi Pandey
Department of ECE, CET, Mody University, Lakshmangarh (332311), India

Rajashree Dutta
Department of ECE, CET, Mody University, Lakshmangarh (332311), India

Ranjana Thalore
Department of ECE, CET, Mody University, Lakshmangarh (332311), India

Abstract

Many emerging applications that need packet delivery from one or more senders to multiple receivers are benefited by Group communication in wireless networks. Due to insecure wireless channels, group communications are prone to various kinds of attacks. Although a number of proposals have been said to secure group communications, provisioning security in group communications in wireless networks, it still remains a critical and challenging issue. This article presents a survey of recent advances in security requirements and services in group communications in two types of wireless networks, and discusses challenges in designing secure group communications in these networks: mobile ad hoc networks, and wireless sensor networks.

Key words – Group communication, attacks, secure group communication, authentication.

I. INTRODUCTION

Group communications refers to either point-to-multipoint or multipoint-to-multipoint communications. A point-to-multipoint communication is the one in which a packet is delivered from a group member to the other members. Whereas, multipoint-to-multipoint communications is the one in which packets are sent via multiple members to other existing members simultaneously. The characteristics of different wireless networks such as ad hoc networks (AHNs), and wireless sensor networks (WSNs), are vastly different in terms of packet types, group managements and resources. One common risk in these networks is that all the members communicating through the wireless channels are more insecure and susceptible to numerous attacks as compared to wired networks [1-3]. Thus, an attempt to establish secure group communications (SGC) over these networks faces various challenges in order to meet security requirements as specified in Table 1.

Table 1. Various characteristics of possible attacks on SGC over wireless networks.

Characteristics/ Network	Mobile ad hoc networks	Wireless sensor networks
Central Authority	No	Yes (base stations/data aggregation nodes)
Storage	Varying	High/very low (base stations/sensors)
Power Supply	Varying	Low
Handoff	No (in IPv4)	Not likely
Mobility (dynamic membership)	High	Varying (likely fixed)
Network Topology	Highly dynamic	Varying
Message Length	Varying (depending on applications)	Relatively short and aggregated
Connectivity	Likely short lived	Either shortly periodic or continuous
Direction of	Duplex	Uniplex for most communications.

connections between a member and a designated controller	(A member is a designated controller)	Duplex only in certain incidents. (A sensor node is an aggregator)
Key Management	Distributed/contributory	Distributed/contributory
Some known attacks	Denial of service, insider, traffic analysis, collusion, routing, Sybil, identity, replay, wormhole, jamming, sinkhole.	Single point of failure, collusion, insider, denial of service, traffic analysis, routing, identity, replay, Sybil, sinkhole, jamming, denial of sleep, denial of service on sensing, node capture.

II. KNOWN ATTACKS IN WIRELESS NETWORKS

Here, we present some known attacks (discussed in later topics and sparsely discussed in [2-5] and some other references) that pose a significant threat to group communications over wireless networks, and categorize these attacks based on their impacts, which include data integrity and confidentiality, power consumption, routing etc.
The known attacks are:

- Data integrity and confidentiality-related attacks.
- Service availability and bandwidth consumption related attacks.
- Routing related attacks.
- Power consumption related attacks.
- Identity related attacks.
- Privacy related attacks.

1. Data integrity and confidentiality-related attacks:

In broad terms, this type of attack tries to disclose or compromise the integrity and confidentiality of data contained in the transmitted data packets.

1.1. ***Denial of service on sensing (DoSS) attack****:* An attacker meddles with data before it is read by sensor nodes, hence resulting in false readings and eventually leading to a wrong decision. A DoSS may attack generally targets physical layer applications in an environment where sensor nodes are located.

1.2. ***Node capture attack:***In this scenario an attacker physically captures sensor nodes and compromises them such that sensor readings sensed by compromised nodes are inaccurate or influenced. In addition, the attacker may try to extract essential cryptographic keys from wireless nodes that are employed to protect communications in most wireless networks.

1.3. ***Eavesdropping attack:***An attacker surreptitiously eavesdrops on ongoing communications between the targeted nodes to collect information on connection and cryptography. We group this attack into this category due to its severe consequences in the sense that the collected cryptographic information may break the encryption keys so that the attacker can retrieve meaningful data.

2. Power consumption related attacks:

This type of attack attempts to exhaust the device's power supply, which is one of the most valuable assets in wireless networks. The worst case may cause a collapse of network communications.

2.1. ***Denial of sleep attack:***An attacker may attempt to drain a wireless device's limited power supply (mostly sensor devices) so that the node's lifetime is considerably shortened. Usually, during a sleep period in which there is no radio transmission, the MAC layer protocol lessens the node's power consumption by regulating the node's radio communications.

3. Service availability and bandwidth consumption related attacks

These attacks can, also be categorized as Power consumption-related attacks. However, since they mainly aim to overwhelm the forwarding capacity of forwarding nodes or put away sparsely available bandwidth, they are more likely related to the service availability and bandwidth consumption concerns. If these attacks result in a denial of service to legitimate members, and might also be referred to as a variant of Denial-of-service (dos) attacks.

3.1. ***Floodicharang attack:***An attacker typically sends a large number of packets to the access point or a victim to avert the victim or the whole network from establishing or continuing communications.

3.2. ***Jamming (radio interference) attack:***An attacker can efficiently cut off wireless connectivity among nodes by transmitting continuous Radio signals such that other authorized users are denied from accessing a particular frequency Channel.

3.3. ***Replay attack:***An attacker copies the forwarded packet and later sends out the copies repeatedly and continuously to the victim to exhaust the victim's buffers or power supplies and access points in order to degrade network performance.

3.4. ***Selective forwarding attack*****:** A forwarding node selectively drops packets that have been originated or forwarded by certain nodes, and forwards other irrelevant packets instead.

4. Routing related attacks:
These attacks attempt to change the routing information, and also manipulate and benefit from such a change in various ways.

4.1. ***Unauthorized routing update attack:***An attacker will attempt to update routing information maintained by routing hosts, such as base stations, access points, or data aggregation nodes, exploit the routing protocols, fabricate the routing update messages, and also might falsely update the routing table.

4.2. ***Wormhole attack:***An adversary intercepts communications originated by the sender, copies a portion of or a whole packet, and speeds up sending the copied packet through a particular *wormhole tunnel* such that the copied packet arrives at the destination earlier than the original packet traversed through normal routes.

4.3. ***Sinkhole attack:***An attacker attracts all nodes to send all packets through one or several of its plotting nodes, called sinkhole node(s), so that the attacker (and its colluding group) has access to all traversing packets.

5. Identity related attacks
Such attacks collaborate with eavesdropping attacks or other network-sniffing software in order to obtain vulnerable network and MAC addresses. They target the authentication entity.

5.1. ***Impersonate attack:***An attacker impersonates another node's identity (either MAC or IP address) to launch or to establish a connection with other attacks on a victim.

5.2. ***Sybil attack:***A single node presents itself to other nodes with multiple spoofed identifications (either MAC or network addresses). The attacker impersonates other nodes' identities or simply create numerous random identities in the MAC orthe network layer. Then the attack poses threats to the other protocol layers; for instance, packets traversed on a route consisting of fake identities are selectively modified or dropped.

6. Privacy related attacks
In general, this type of attack exposes the anonymity and privacy of communications and, in worst case scenarios, can cause false accusations of an innocent victim.

6.1.1. ***Traffic analysis attack:***An attacker might gain knowledge of the network, traffic, and nodes' behaviors. The traffic analysis may involve observing the message length, message coding or pattern, and duration for which the message stayed in the router. In addition, the attacker can correlate all outgoing and incoming packets at any router or any member. Such an attack violates privacy and can harm members for being linked with messages.

III. SECURE GROUP COMMUNICATION SYSTEMS

A Group Communication System (GCS) consists of the following five common operations: initiate, join, leave, partition, and merge. The group is first established by initial members. Then one or several potential members join the group while some members leave the group. This is so-called dynamic membership. A large number of membership changes, referred to as a bulk membership change, may require a specialized protocol design without demeaning group performance. In some scenarios a group can be divided into smaller subgroups or fused into a bigger group. This is also considered as a bulk membership change, but the transitions among groups likely incur overheads. This dynamic membership aspect requires the Group Communication Systems to rekey the session keys in order to preserve the key secrecy.

1. Security requirements and security services in secure group communications:

This part discusses security requirements and corresponding security services in securing group communications and alleviating attack. Many systems have been proposed to address the requirements and provide such services, but only a few promising systems are presented here.

1.1. Group Key Management (GKM)*:*The fundamental security service in SGC is the provision of a shared key, the group key. The shared group key is used to encrypt a group message, authenticate members and messages, sign the message, and authorize access to traffic and group resources. A Group Key Management scheme used in any secure group communication system should satisfy the following requirements:

- Imitation of the group key should be infeasible or computationally difficult.
- Key generation is secure.
- The group key is securely distributed and only the legitimate users can receive a valid group key.
- A rekeying of the key is secure.
- Revocation of the group key upon every membership change should be immediate.

1.2. Group authentication*:* In group communication (one-to-many and many-to-many), a member can be the designated sender, the designated receiver, or both. Both the users and the messages should be authenticated in order to safeguard identity related attacks.

1.3. Group authorization and access control*:* In any conventional access control mechanism, a member who holds a decrypting key can access full contents in a flow (or all flows in an aggregated stream). This is referred to as a single access privilege. The stream should be accessed with different access privileges such that only members who have an appropriate privilege can access the corresponding portions of contents (or flows). This is referred to as multiple access privilege.

1.4. Group accounting and nonrepudiation*:*Any group operation executed or a record of resources utilized by a member should be available for tracking in order to detect any abusive usage of resources and operations. In general, the group

Table 2. Security services to countermeasure attacks.

Attacks	Security services to counter attacks					
	Authentication	**Authorization/ access control**	**Accounting/ Non-repudiation**	**Message confidentiality and integrity**	**Privacy/ anonymity**	**Survivability/ availability**
Node capture	—	Username, password, ID	—	e{management & data} & hash	—	Node intrusion detection
Denial of sleep	Source & message authentication	Access control on routing table	group signature	e{management} & hash	—	—
Denial of service on sensing	—	—	—	—	—	Sensing tampering detection
Eavesdropping	—	—	—	e{management & data} & hash	Source–destination anonymity	—
Flooding	Source authentication	—	—	—	—	Early detection for excessive amount of packets
Jamming	—	—	—	e{data} & hash	—	Jamming detection
Replay	—	—	Group signature, packet sequence number and timestamp	e{data with nonce} & hash	—	—
Selective Forwarding	Source & message authentication	—	Group signature, timestamp, and packet sequence number	e{data with nonce} & hash	—	—
Unauthorized routing update	Source & message authentication	Access control on routing table	Message signature	e{management} & hash	—	Loophole and sinkhole routing detection
Wormhole	Source authentication	access control on routing table and using directional antenna	—	e{management, data with nonce} & hash	—	—

signature and member certificate can be used to authenticate the source and message, and to provide proof of the source's activity in case of a dispute.

1.5. Group privacy and anonymity*:* Any information related to a group message, such as identities of a receiver and a sender, message time and length, can be protected or hidden to preserve privacy and anonymity of members.

1.6. Group message integrity and confidentiality*:*
Message integrity should be well-maintained by ensuring that the message has not been fabricated or dropped by an unauthorized entity. This can be done by several means, which includes hashing and signing the message beside strong encryption keys.

1.7. Group survivability and availability*:*An attacker can attack routing hosts to isolate some or all group members, or partition the group. Thus, the entire routing hosts must be protected in order to ensure group survivability. However, the attacker can still target a joining procedure (i.e., by flooding the access point or base station in wireless infrastructure networks and WSNs), thus causing service unavailability to other legitimate users.

Impersonate	Source authentication	Access control list	Group signature and time-expired certificate	e{management & data} & hash	—	—
Sinkhole	Source & message authentication	Access control on routing table	—	e{management} & hash	—	—
Sybil	Source authentication	Access control list	Group signature and time-expired certificate	e{management & data} & hash	—	Detection of Multiple IDs
Traffic Analysis	Message authentication	—	Group signature, timestamp, and packet sequence number	e{data} & hash	Source–destination anonymity	—

IV. SGC OVER MOBILE AD HOC NETWORKS

Some SGCs that provide security protection specifically over mobile ad hoc networks are surveyed in this section.

1. Kaya *et al.* [11] suggested a dynamic multicast group management protocol that tries to equally distribute the workload of securing communications to all participating members.

PROS	CONS
Communication overheads and latency of linking revocation processes do not significantly degrade the group performance as the number and speed of joining/leaving nodes increase.	The scheme did not discuss how the group manager is selected as well as the transitions of group information between the new and old group managers.

2. Striki and Baras [9] presented a Merkle tree based user authentication scheme by constructing dynamic distributed central authorities (CAs) based on Merkle trees, and then equipping these CAs with two key generation protocols: 2d-Octopus and Tree-Based Group Diffie-Hellman (TGDH)-based 2d-Octopus. It has been emphasized that incorporating user authentication and key distribution algorithms in a collaborative manner into SGC yields a scalable and efficient key management protocol in MANET's.

PROS	CONS
The modified Merkle tree-based scheme with TGDH-based 2d-Octopus has lower communication and processing overheads than that with 2d-Octopus and another existing protocol, one-way function tree (OFT), as the size of the group increases.	The scheme does not talk over how this integration of authentication and key distribution could better protect SGC against various threats, such as DoS and collusion attacks.

3. Balachandran *et al.* [10] proposed a key agreement scheme for SGC over MANETs, stated to as the Chinese Remainder Theorem and Diffie-Hellman (CRDTH) scheme, which purposes to solve two problematic issues in ad hoc environments: key serialization and absence of a central authority in MANETs. The key management in this scheme is a contributory-based GKM. All members exchange their contributed key share by using the Diffie-Hellman key exchange mechanism, and then the members independently but communally generate the group key that is based on the Chinese remainder theorem (CRT).

PROS	CONS
The scheme can equally distribute the computational workloads to all members. It involves only one round of broadcast to rekey the group key for a leaving process and two rounds for an initial key formation process(during group formation) and a joining process.	The authors only suggested how the scheme would be compromised rather than validating the security of the scheme

V. SGC OVER WIRELESS SENSOR NETWORKS

1. Zhu *et al.* [6] proposed a key management protocol, known as localized encryption and authentication protocol (LEAP), used for large-scale distributed sensor networks. The protocol is designed based on two interpretations: first, different packet types exchanged among sensor nodes require different security services, and second, a single key management scheme may not be suitable for various security requirements.

PROS	CONS
Low communication overheads; the scheme is energy efficient.	The scheme did not discuss the power consumption of sensor nodes in deploying some of the proposed security mechanisms.

2. Yu and Guan [7] proposed a group-based key pre distribution scheme by partitioning the network into hexagonal grids with a specified size. Nodes are then divided into groups, and each group is placed into a grid such that the number of neighbors of a node is minimized, thereby reducing power consumption. The scheme classifies communications of sensor nodes into two types: intergroup and in-group.

PROS	CONS
The scheme provisions a high degree of connectivity, which is defined as the fraction of the size of the largest connected components over the size of the entire sensor network.	The optimal grid size may not be precisely determined, thus possibly resulting in two incidents: the inter-group keys may not be generated if the grid size is too small, and the power consumption is relatively high if the grid size is too large.

3. Zhang and Cao [8] proposed a set of pre-distributed and local collaboration-based group rekeying (PCGR) schemes to mitigate the node capture attack and the DoSS attack. Thus, the future keys must be protected by encryption with some polynomials, which are kept by someone-hop neighboring nodes.

PROS	CONS
The schemes can effectively protect SGC against node capture and DoSS attacks.	Rekeying is very limited due to a limited number of reusable future keys.

4. Huang *et al.* [13] proposed a secure level key infrastructure for multicast (SLIMCAST) to protect data confidentiality via hop-by-hop re-encryption and mitigate the DoS-based flooding attack through intrusion detection and deletion mechanism. The SLIMCAST protocol splits a group routing tree into levels and branches in a bundled manner. Communications among nodes in each level in each branch of the group tree are protected by a level key such that only the local level key is rekeyed during joining and leaving processes

PROS	CONS
Low communication overheads and power consumption. Performance does not substantially degrade as the group size increases.	The performance is degraded (i.e., high power consumption) when membership changes are massive.

VI. CONCLUSION

The number of applications of group communications over wireless networks keeps on increasing, such as group-oriented military systems and education systems. However, communications over wireless channels is, by nature, insecure and easily susceptible to various kinds of attacks. We have discussed known attacks that can severely disrupt group communications in wireless networks. Next, we have shown necessary security requirements, and alsodemonstrated fundamental security services to meet these requirements and safeguard the communications against such attacks. We have demonstrated that many attacks can be prevented and diminished by the proposed security services. With respect to limited computation capability and scarce wireless channels, these works basically attempt to reduce communication and processing overheads, and to fend off some particular attacks.

Schemes	Mobile ad hoc networks				Wireless sensor networks				
Characteristics	[11]	[9]	[10]	[14]	[6]	[7]	[8]	[15]	[2]
Key management	Ad hoc group key (AGK)	Tree-based group Diffie-Hellman (TGDH)	Chinee Remainder and Diffie-Hellmn	Routing aware key distribution	Cluster based keys	Group based key	Locally Group based key and key pre-distribution	Cluster based tree (level and branch)	N/A

Authentication	Certificate based PK2 auth.	ID-based User auth. & Merkle tree-based data auth.	N/A	N/A	Source and Message one-way keychain based and challenge response auth.	N/A	N/A	MAC sig. and one way sequence number	N/A
Accounting/ nonrepudiation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	N/A
Authorization / access control	Certificate	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Privacy/ anonymity	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes (virtual infrastructure)
Message integrity and confidentiality	Yes	Yes	Yes	Yes	N/A	N/A	N/A	Yes	N/A
Survivability/ availability	Yes (quick recovery)	Yes	N/A	N/A	Yes	Yes	Yes	N/A	Yes
Attack prevention[3]	Message modification, replay	Impersona, collusion	N/A	N/A	Wormhole, sinkhole, Sybil, DoS, replay, insider	Node captu re	Node capture, eavesdropping, DoSS	Node capture, Sybil	DoS, traffic analysis
Reducing communication overheads	Yes (using locality to reduce comm. complexity)	Yes	N/A	Yes	Yes (using locality to reduce comm. Complexity)	N/A	Yes	Yes	Yes
Reducing processing overheads	N/A	Yes	Yes	N/A	Yes	N/A	Yes	Yes	N/A
Handling high mobility	Yes	N/A	Yes	Yes	N/A	N/A	N/A	Yes	N/A
Steady performane	Yes	Yes	N/A	Yes	N/A	N/A	N/A	Yes	N/A

vs.groupsize									
Scalable	Yes	Yes	Yes	Yes	N/A	N/A	N/A	Yes	Yes
Energy-efficient	N/A	N/A	N/A	Yes	N/A	N/A	N/A	Yes	Yes

1 N/A: Information not available about the characteristic OR the characteristic is not likely possible or not applicable.

2 PK: Public key.

3 Only specified attacks discussed in the respective references are listed here even though each of these schemes may mitigate other attacks as well.

Table 3. Comparison of SGC over wireless networks.

REFERENCES

[1] S. K. S. Gupta and S. Cherukuri, "An Adaptive Protocol for Efficient and Secure Multicasting in IEEE 802.11 Based Wireless LANs," Proc. IEEE WCNC 2003, vol. 3, Mar. 2003, pp. 2021–26.
[2] A. Wadaa et al., "On Providing Anonymity in Wireless Sensor Networks," Proc. 10th Int'l. Conf. Parallel and Distrib. Syst., July 2004, pp. 411–18.
[3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Elsevier's Ad Hoc Networks J., Special ssueI on Sensor Network Applications Protocols, vol. 1, no. 2–3, Sep. 2002, pp. 293–315.
[4] R. Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc. IEEE INFOCOM '07, Mar. 2007.
[5] B. Decleene et al., "Secure Group Communications for Wireless Networks," Proc. IEEE MILCOM 2001, vol. 1, Oct. 2001, pp. 113–17.
[6] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc. 10th ACM Conf. Computer and Commun. Security, Oct. 2003, pp. 62-72.
[7] Z. Yu and Y. Guan, "A Robust Group-Based Key Management Scheme for Wireless Sensor Networks," Proc. IEEE WCNC '05, vol. 4, Mar. 2005, pp. 1915–20.
[8] W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Networks: a Predistribution and Local Collaboration-Based Approach," Proc. IEEE INFOCOM'05, vol. 1, Mar. 2005, pp. 503–14.
[9] M. Striki and J. Baras, "Towards Integrating Key Distribution with Entity Authentication for Efficient, Scalable and Secure Group Communication in MANETs," Proc. IEEE ICC '04, vol. 7, June 2004, pp. 4377–81.
[10] R. K. Balachandran et al., "CRTDH: An Efficient Key Agreement Scheme for Secure Group Communications in Wireless Ad Hoc Networks," Proc. IEEE ICC '05, vol. 2, May 2005, pp. 1123–27.
[11] T. Kaya et al., "Secure Multicast Groups on Ad Hoc Networks," Proc. ACM SASN '03, Oct. 2003, pp. 94–103.
[12] L. Lazos and R. Poovendran, "Cross-Layer Design for Energy-Efficient Secure Multicast Communications in Ad Hoc Networks," Proc. IEEE ICC 2004, vol. 6, June 2004, pp. 3633–39.
[13] J.-H. Huang, J. Buckingham, and R. Han, "A Level Key Infrastructure for Secure and Efficient Group Communication in Wireless Sensor Networks," Proc. 1st Int'l. Conf. on Security and Privacy for Emerging Areas in Commun. Net., Sep. 2005, pp. 249–60.