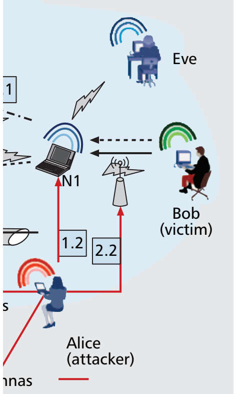
SECURITY IN WIRELESS
MOBILE AD HOC AND SENSOR NETWORKS

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

PITIPATANA SAKARINDR AND NIRWAN ANSARI, NEW JERSEY INSTITUTE OF TECHNOLOGY



The authors present a survey of recent advances in security requirements and services in group communications in three types of wireless networks, discussing challenges in designing secure group communications in these networks.

ABSTRACT

Group communications in wireless networks has been facilitating many emerging applications that require packet delivery from one or more sender(s) to multiple receivers. Due to insecure wireless channels, group communications are susceptible to various kinds of attacks. Although a number of proposals have been reported to secure group communications, provisioning security in group communications in wireless networks remains a critical and challenging issue. This article presents a survey of recent advances in security requirements and services in group communications in three types of wireless networks, and discusses challenges in designing secure group communications in these networks: wireless infrastructure networks, mobile ad hoc networks, and wireless sensor networks.

INTRODUCTION

Group communications refers to either point-to-multipoint (in which a packet is delivered from a group member to the other members) or multipoint-to-multipoint communications (in which packets are sent from multiple members to other members simultaneously). The characteristics of different wireless networks — wireless infrastructure networks (WINs), ad hoc networks (AHNs), and wireless sensor networks (WSNs) — are vastly different in terms of group management, packet types, and resources. However, one common risk among these networks is that all members communicating through wireless channels are more insecure and susceptible to numerous attacks than 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.

The rest of the article is organized as follows. First, various known attacks are presented, followed by a discussion on group communications, and security requirements and services in securing group communications. Several proposals for SGC over these different networks are then discussed.

KNOWN ATTACKS IN WIRELESS NETWORKS

Here, we present some known attacks (intensively discussed in [2–5] and sparsely discussed in other references) that pose a significant threat to group communications over wireless networks, and categorize these attacks based on their impacts, including data integrity and confidentiality, power consumption, routing, identity, privacy, and service availability. For example, Figs. 1 and 2 illustrate some of these attacks in a real wireless network.

DATA INTEGRITY AND CONFIDENTIALITY-RELATED ATTACKS

In general, this type of attack attempts to reveal or compromise the integrity and confidentiality of data contained in the transmitted packets.

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

Node capture attack: An attacker physically captures sensor nodes and compromises them such that sensor readings sensed by compromised nodes are inaccurate or manipulated. In addition, the attacker may attempt to extract essential cryptographic keys (e.g., a group key) from wireless nodes that are used to protect communications in most wireless networks.

Eavesdropping attack: An attacker secretly eavesdrops on ongoing communications between targeted nodes to collect information on connection (e.g., medium access control [MAC] address) and cryptography (e.g., session key materials). Although this attack can be classified into other categories such as privacy-related

1536-1284/07/$20.00 © 2007 IEEE

Networks Characteristics	Wireless infrastructure networks	Mobile ad hoc networks	Wireless sensor networks
Central authority	Yes	No	Yes (base stations/data aggregation nodes)
Computation	High/varying (basestations/devices)	Varying	High/very low (base stations/sensors)
Storage	High/varying (basestations/devices)	Varying	High/very low (base stations/sensors)
Power supply	High	Varying	Low
Handoff	Yes	No (in IPv4)	Not likely
Mobility (dynamic membership)	Varying	High	Varying (likely fixed)
Network topology	Varying (likely low dynamic)	Highly dynamic	Varying (likely highly dynamic due to short life cycles and unreliability of nodes)
Message length	Varying (depending on applications)	Varying (depending on applications)	Relatively short and aggregated
Connectivity	Continuous	Likely short lived	Either shortly periodic or continuous
Direction of connections between a member and a designated controller	(A member — an access point) Duplex	(A member — a designated controller) Duplex	(A sensor node — an aggregator) Uniplex for most communications Duplex only in certain incidents (e.g., locating the aggregator)
Key management	Centralized/contributory	Distributed/contributory	Distributed/contributory
Predetermined information	Possible	Limited–not at all	Most likely
Potential cryptography	Varying	Varying	Symmetric/elliptic curve cryptography (ECC)
Additional criteria	1. Key management and dynamic membership during a handoff period.	1. All network and key management tasks should be equally distributed (fairness). 2. Network partitions can occur more frequently and may increase the number of isolated nodes. 3. Multicast routings are updated frequently due to a dynamic network. 4. Trust relationship can enhance the performance.	1. The ratio of the length of encrypted messages to messages should be as low as possible. 2. Trust relationship can enhance the performance.
Some known attacks	Single point of failure (at access points), denial of service, collusion, insider, traffic analysis, routing, identity, replay, jamming.	Denial of service, collusion, insider, traffic analysis, routing, identity, replay, jamming, Sybil, wormhole, sinkhole.	Single point of failure (at base stations/data aggregating nodes), denial of service, collusion, insider, traffic analysis, routing, identity, replay, jamming, Sybil, sinkhole, denial of sleep, denial of service on sensing, node capture.

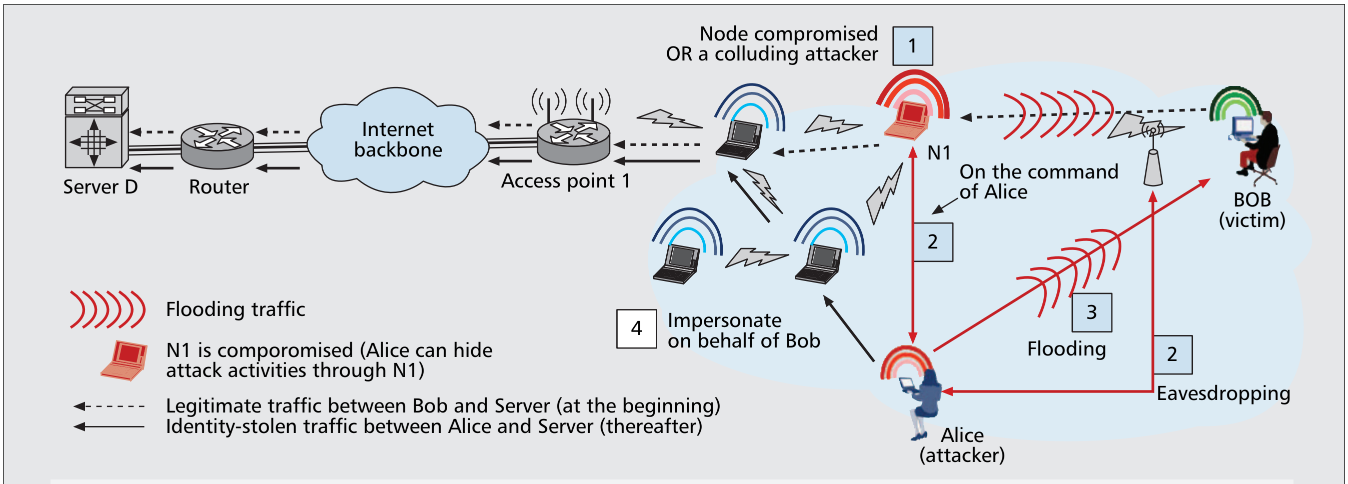
Table 1. *Characteristics of possible attacks on SGC over wireless networks.*

attacks, we group it into this category due to its severe consequences in the sense that the collected cryptographic information may break the encryption keys such that the attacker can retrieve meaningful data.

Power Consumption Related Attacks

In general, 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 would cause a collapse of network communications.

Denial of sleep attack: An attacker tries to drain a wireless device's limited power supply (especially sensor devices) so that the node's lifetime is significantly shortened. In general, during a sleep period in which there is no radio transmission, the MAC layer protocol reduces the node's power consumption by regulating the node's radio communications. Thus, the attacker


Node compromised
OR a colluding attacker
1
Internet backbone
Server D
Router
Access point 1
N1
On the command of Alice
2
BOB (victim)
Flooding traffic
N1 is comporomised (Alice can hide attack activities through N1)
Legitimate traffic between Bob and Server (at the beginning)
Identity-stolen traffic between Alice and Server (thereafter)
4
Impersonate on behalf of Bob
3
Flooding
2
Eavesdropping
Alice (attacker)

Scenario: Bob communicates with a data-sensitive server through hybrid (infrastructure/ad hoc) wireless networks.
Attacks: Eavesdropping, impersonate, flooding, and collusion.
Steps:
1A. Alice has previously compromised N1 by any means.
1B. Alternatively, N1 is a colluding attacker that shares information and helps to carry out the attack.
2. Alice may command N1 to start eavesdropping on Bob's incoming and outgoing packets. If possibly, Alice may eavesdrop on N1 packets due to insecure wireless channel. This eavesdroppping attack aims to collect more information about Bob's communication with the server D for traffic analysis.
3. Alice floods Bob's machine or network such that Bob is denied of service. Note that Alice is unlikely to ask a colluding N1 to launch the flooding attack because N1 will possibly be caught.
4. Alice impersonates Bob's identity to falsely gain access, on behalf of Bob, to information authorized by server D to Bob. Note that Bob cannot notify server D due to the effect of the flooding attack and we assume that Bob does not use an out-of-bound channel (e.g. telephone to the server D's operator).

Figure 1. *An illustration of mixed attacks in a real wireless network.*

attacks the MAC layer protocol to shorten or disable the sleep period. If the number of power-drained nodes is large enough, the whole sensor network can be severely disrupted.

Service Availability and Bandwidth Consumption Related Attacks

These attacks can, in fact, also be categorized as power consumption-related attacks. However, since they mainly aim to overwhelm the forwarding capability of forwarding nodes or consume sparsely available bandwidth, they are more likely related to the service availability and bandwidth consumption concerns, they are highlighted in this category. If these attacks result in a denial of service to legitimate members, they can also be referred to as a variant of denial-of-service (DoS) attacks.

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

Jamming (radio interference) attack: An attacker can effectively cut off wireless connectivity among nodes by transmitting continuous radio signals such that other authorized users are denied from accessing a particular frequency channel. The attacker can also transmit jamming radio signals to intentionally collide with legitimate signals originated by target nodes.

Replay attack: An attacker copies a forwarded packet and later sends out the copies repeatedly and continuously to the victim in order to exhaust the victim's buffers or power supplies, or to base stations and access points in order to degrade network performance. In addition, the replayed packets can crash poorly designed applications or exploit vulnerable holes in poor system designs.

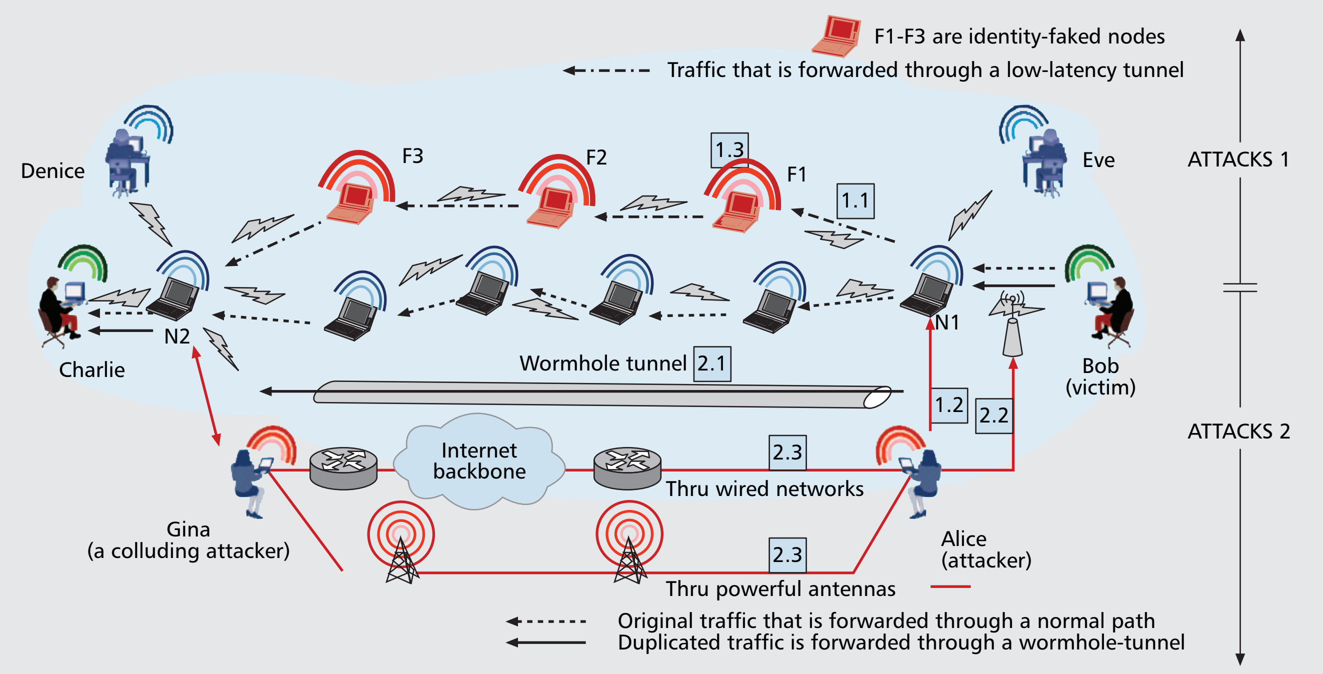
Selective forwarding attack: A forwarding node selectively drops packets that have been originated or forwarded by certain nodes, and forwards other irrelevant packets instead.

Routing Related Attacks

In general, these attacks attempt to change routing information, and to manipulate and benefit from such a change in various ways.

Unauthorized routing update attack: An attacker attempts to update routing information maintained by routing hosts, such as base stations, access points, or data aggregation nodes, to exploit the routing protocols, to fabricate the routing update messages, and to falsely update the routing table. This attack can lead to several incidents, including: some nodes are isolated from base stations; a network is partitioned; messages are routed in a loop and dropped after the time to live (TTL) expires; messages are perversely forwarded to unauthorized attackers; a black-hole route in which messages are maliciously discarded is created; and a previous key is still being used by current members because the rekeying messages destined to members are misrouted or delayed by false routings.

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 specialized *wormhole tunnel* such that the copied packet arrives at the destination earlier than the original packet traversed through normal routes. The wormhole tunnel can be created by several


F1-F3 are identity-faked nodes
Traffic that is forwarded through a low-latency tunnel
Denice
F3
F2
1.3
F1
1.1
Eve
ATTACKS 1
N2
Charlie
N1
Bob
(victim)
Wormhole tunnel
2.1
1.2
2.2
ATTACKS 2
Internet
backbone
2.3
Thru wired networks
Gina
(a colluding attacker)
2.3
Alice
(attacker)
Thru powerful antennas
Original traffic that is forwarded through a normal path
Duplicated traffic is forwarded through a wormhole-tunnel

Scenario: Bob (and Denice) communicates with Charlie (and Eve) through a mobile ad hoc network.

Attacks 1: Sybil, sinkhold, and selectively forwarding attacks.

Steps:
1.1 Alice generates multiple fake identifications, and advertises an attractive "low-latency" path consisting of these identities to N2. (Sybil attack)
1.2 Alice advertises this low-latency path to N1, who updates its routing table accordingly. N1 forwards Bob's packets to Charlie through this low-latency path. (Sinkhole attack)
1.3 Alice passively eavesdrops all Bob-Charlie's packets or selectively drops all Bob-Charlie's packets while still forwarding Denice-Eve's packets to reduce the possibility of being caught. (Selectively forwarding attack)

Attacks 2: Eavesdropping, wormhole, false routing, and collusion attacks.

Steps:
2.1 Alice sets up a wormhole tunnel (in this illustration, either thru wired networks or thru powerful antennas) to Gina, a colluding attacker. (Collusion attack)
2.2 Alice eavesdrops Bob-N1's packets and copies them. (Eavesdropping attack)
2.3 Alice forwards the copies to Gina through the wormhole tunnel. (Wormhole attack)
2.4 Gina forwards the copies to N2. N2 updates the new route between N1 and N2 through this wormhole tunnel. (False routing update)

Figure 2. *An illustration of routing related and other attacks.*

means, such as by sending the copied packet through a wired network and at the end of the tunnel transmitting over a wireless channel, using a boosting long-distance antenna, sending through a low-latency route, or using any out-of-bound channel, as illustrated in Fig. 2. The wormhole attack poses many threats, especially to routing protocols and other protocols that heavily rely on geographic location and proximity, and many subsequent attacks (e.g., selectively forwarding, sinkhole) can be launched after the wormhole path has attracted a large amount of traversing packets. Readers are referred to [4] for details and a mechanism to detect such an attack.

Sinkhole attack: An attacker attracts all nodes to send all packets through one or several of its colluding nodes, called sinkhole node(s), so that the attacker (and its colluding group) has access to all traversing packets. To attract the victimized nodes, the sinkhole node is usually presented as an attractive forwarding node such as having a higher trust level, being advertised as a node in the shortest distance or short delay path to a base station, or a nearest data aggregating node (in WSNs).

Identity Related Attacks

In general, these attacks cooperate with eavesdropping attacks or other network-sniffing software to obtain vulnerable MAC and network addresses. They target the authentication entity.

Impersonate attack: An attacker impersonates another node's identity (either MAC or IP address) to establish a connection with or launch other attacks on a victim; the attacker may also use the victim's identity to establish a connection with other nodes or launch other attacks on behalf of the victim, as illustrated in Fig. 1. There are several softwares capable of reprogramming the devices to forge the MAC and network addresses.

Sybil attack: A single node presents itself to other nodes with multiple spoofed identifications (either MAC or network addresses). The attacker can impersonate other nodes' identities or simply create multiple arbitrary identities in the MAC and/or network layer. Then the attack poses threats to other protocol layers; for examples, packets traversed on a route consisting of fake identities are selectively dropped or modified; or a threshold-based signature mechanism that relies on a specified number of nodes is corrupted.

A GCS consists of five common operations: initiate, join, leave, partition, and merge. The group is first established by initial members. Then, one or several prospective members join the group while some members leave the group. This is the so-called dynamic membership.

PRIVACY RELATED ATTACKS

In general, this type of attack uncovers the anonymity and privacy of communications and, in the worst case, can cause false accusations of an innocent victim.

Traffic analysis attack: An attacker attempts to gain knowledge of the network, traffic, and nodes' behaviors. The traffic analysis may include examining the message length, message pattern or coding, and duration the message stayed in the router. In addition, the attacker can correlate all incoming and outgoing packets at any router or member. Such an attack violates privacy and can harm members for being linked with messages (e.g., religious-related opinions that are deemed provocative in some communities). The attacker can also perversely link any two members with any unrelated connections.

If a group of attackers collude to launch any type of attacks, it is referred to as a collusion attack. For example, the colluding group of attackers orchestrates to collect information to significantly exploit the system, masquerade a legitimate member and send out fault messages on behalf of that member, conjointly mount attacks against other members or network entities, or falsely accuse a legitimate member as an attacker.

SECURE GROUP COMMUNICATION SYSTEMS

A group communication system (GCS) consists of five common operations: initiate, join, leave, partition, and merge. The group is first established by initial members. Then one or several prospective 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, require a specialized protocol design without degrading group performance. In some scenarios a group can be partitioned into smaller subgroups or merged into a bigger group. This can also be considered a bulk membership change, but the transitions among groups likely incur overheads. This dynamic membership aspect requires the GCS to rekey the session keys in order to preserve the key secrecy. For WSNs, this dynamic membership may not be necessary because the keys are most likely predetermined prior to deployment [6–8]. In wireless infrastructure and ad hoc networks, most, if not all, GKM schemes require each member to keep the membership list, thus incurring huge communication overhead. However, in a WSN, this list might not be necessary due to storage limitations of sensor nodes and the provision of preselected entities (data aggregating nodes) to keep track of their members.

SECURITY REQUIREMENTS AND SECURITY SERVICES IN SGC

This section discusses security requirements and corresponding security services in securing group communications and mitigating attacks as summarized in Tables 1 and 2. Table 3 describes in depth the characteristics of major security services over wireless networks. Many systems have been proposed to address the requirements and provide such services, but only a few promising systems are presented here due to space limits.

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, sign the message, authenticate members and messages, and authorize access to traffic and group resources. Thus, the strength of SGC largely relies on the cryptographic strength of the keys and the key management protocol. A GKM scheme deployed in any secure group communication system should satisfy the following requirements:

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

Basically, GKM can be categorized into three types based on how the key is generated: centralized, distributed, and contributory [9, 10]. A revocation can be performed by limiting the session period for which the keys are valid. Then the session period and remaining period are calculated and attached along with keys before being distributed to all members. If keys need to be rekeyed (with three triggering conditions as discussed in Table 3), the key revocation can be sent by the designated entity to notify all members holding these keys, as discussed in [6, 11].

Group authentication: In group communication (one-to-many and many-to-many), a member can be either the designated sender, the designated receiver, or both. Both users and messages should be authenticated to safeguard identity related attacks. In some systems a member certificate is issued by the trusted certificate issuing entity along with its validation period. In some systems the expired certificate is maintained for further verifications, as discussed in [9]. Expired certificates are compiled into the revocation list, which is distributed to notify all members.

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. In many group-oriented applications, group members can be assigned with multiple access privileges. Thus, 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.

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. A nonrepudiation service can ensure that the identity of a member whose activities are in dispute can be

Attacks	Security services to countermeasure attacks					
	Authentication	Authorization/ access control	Accounting/ nonrepudiation	Message confidentiality and integrity	Privacy/ anonymity	Survivability/ availability
Denial of service on sensing	—	—	—	—	—	Sensing tampering detection
Node capture	—	Username, password, ID	—	e{management & data} & hash	—	Node intrusion detection
Eavesdropping	—	—	—	e{management & data} & hash	Source–destination anonymity	—
Denial of sleep	Source & message authentication	access control on routing table	group signature	e{management} & hash	—	—
Flooding	Source authentication	—	—	—	—	Early detection for an excessive amount of packets
Jamming	—	—	—	e{data} & hash	—	Jamming detection
Replay	—	—	Group signature, timestamp, and packet sequence number	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	—	—
Sinkhole	Source & message authentication	Access control on routing table	—	e{management} & hash	—	—
Impersonate	Source authentication	Access control list	Group signature and time-expired certificate	e{management & data} & hash	—	—
Sybil	Source authentication	Access control list	Group signature and time-expired certificate	e{management & data} & hash	—	Multiple IDs detection
Traffic Analysis	Message authentication	—	Group signature, timestamp, and packet sequence number	e{data} & hash	Source–destination anonymity	—

■ **Table 2.** *Security services to countermeasure attacks.*

fully and precisely determined by the designated entity. In general, the group 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.

Group privacy and anonymity: Any information related to a group message, such as identities of a sender and a receiver, message length, and time, can be protected or hidden to preserve privacy and anonymity of members. An anonymous message refers to a message that carries no information about the senders and receivers.

Group message integrity and confidentiality: Message integrity should be preserved by ensuring that the message has not been fabricated (some or all portions of the message have not been added, deleted, or modified) or dropped by an unauthorized entity. This can be done by sev-

Services	Characteristics			Details
Group key management	Type of key management	Centralized		• A dedicated entity (e.g. a key manager) generates both long-term and short-term keys, distributes them to associated members, and maintains the key material and lists. • The security of key selection and generation is high, but the key manager carries most of workloads and becomes a point of target. • In wireless infrastructure and sensor networks, this central entity can be an access point, a base station, or a dedicated key server. • However, this centralized-based GKM scheme is not applicable to ad hoc networks.
		Partially distributed		• A group is divided into smaller sub-groups. Some members in each subgroup may temporarily function as a key-generating server. • A key manager has a reduced workload. Still, it is a point of target and the security of key generation is compromised. • The distributed-based GKM scheme is applicable to ad hoc and sensor networks, but not to wireless infrastructure networks.
		Contributory		• Without a central key server/manager, each member randomly and independently selects its contribution based on some key-generating algorithms that are agreed upon by all members during the joining process. Then, the contributions are exchanged within a group, and a shared group key is identically generated. • The security of key selection and generation is low, but there is no need for a key manager. All members equally share the workloads. • This GKM type is applicable to ad hoc networks, but not to wireless infrastructure (no center) and sensor networks (the complexity of key generation and overheads are too high).
	Key secrecies	Forward secrecy		• The forward secrecy ensures that a new joining member cannot use the new key to decrypt all messages which have been encrypted with the previous key(s).
		Backward secrecy		• The backward secrecy ensures that a leaving member cannot use the previous key(s) to decrypt all messages encrypted with the new key.
		Perfect forward secrecy		• The perfect forward secrecy ensures that a compromise of a long-term key seed which was used to generate the present short-term key(s) cannot deprive the secrecy of other previous short-term keys which have been generated by the compromised long-term key seed.
	Key independence			• A disclosure of a subset of session keys cannot deprive the secrecy of other subsets of session keys which have been generated by the same long-term key seed.
	Key serialization			• In some distributed and contributory-based GKM schemes, the key materials are selected and the group key is generated by members in an ordered sequence, as discussed in [8]. An attack on any participating member disrupts the whole process. Note that the key materials are actually key seeds used to generate keys (e.g., primes in RSA or DH) • Instead, some schemes may construct the key by other ways, i.e., broadcasting the key materials to all members or establishing a key tree, at the expense of communication and storage overheads. In addition, with insecure wireless channel, these ways may lead to service unavailability especially in ad hoc networks where membership is highly dynamic.
	Rekeying	No. of rekey messages		• An average number of distributed and received messages per member (or per key manager) should be minimized.
		Length of rekey messages		• Some protocols reduce the number of rekey messages by aggregating multiple messages into a single message, which in return increases the consumed bandwidth for one transmission. Thus, the performance metric should also determine the bandwidth consumption per message in addition to the number of transmitted messages.
		Rekeying process		• The rekeying operation should reduce or optimize the computation and time complexity of rekeying operation with respect to a group size.
		Triggering conditions	Membership	• Keys associated with the membership changes must be rekeyed to ensure the key secrecy for the remaining members.
			Periodic	• To provide a better key secrecy, the rekeying operation is invoked periodically to prevent keys from being compromised over time.
			Specified	• A system enables the rekeying operation for specified incidents, such as upon a detection of attacks or violations.
Authentication	Message authentication			• A system should require a sender to sign a message and a receiver to verify such a message signature on its authenticity as well as integrity.
	User authentication			• Users should be authenticated upon joining the group, signing the messages, or accessing group materials.
		Sender viewpoint		• A designated sender may want to multicast a message on behalf of the group to all designated receivers without revealing its real identity.
		Receiver viewpoint		• A receiver verifies whether the message has been originated by an unspecified group member (not an outsider). • OR a receiver verifies whether the message has been originated by an unspecified but designated sender (not an outsider and not designated receivers). • OR, in a possibly disputable case, a receiver verifies whether the message has been originated by the specified and designated sender.

Table 3 continued on next page...

Services	Characteristics		Details
Access control	Authorization/access control techniques		• The group resources (e.g., key seeds, keys, a member list, multicast routing tables, etc.) and group messages should be accessible only to authorized members. • The access control list can be used to determine if the member has permission to access resources and, more specifically, to which resource is accessible.
	Dynamic access control		• A system enables the member to dynamically change its request to access resources. Consequently, the system must be able to update access permissions and restrictions with additional mechanisms when the member's access privilege changes. Other systems may simply give all members a fixed access control privilege per session.
Non-repudiation	Message signature		• A system requires messages to be signed or equipped with a membership certificate so that an originator (signer) of the message can always be identified.
	Timestamp and/or sequence number		• Timestamps and/or sequence numbers can be used to limit a validation of certificate or message signature, and to prevent replay attacks.
	Revocation of certificates		• The expired certificate or misuse of certificate is revoked by the issuer and may be publicly announced in the revocation list. • For higher non-repudiation, some systems may keep the expired certificates for future verification at the expense of storage overhead.
	Characteristics of signature	Unforgeable	• A group of colluded attackers cannot generate a group signature identical to that generated by a legitimate member.
		Non-allegeable	• A group of colluded attackers cannot generate a group signature by which a group controller falsely identifies a legitimate member as an attacker.
		Linkable	• A group of colluded attackers cannot generate a valid group signature by which a group controller cannot identify the identity of any of these attackers.
		Secretive	• A member's secret elements can neither be retrieved from a group signature nor from any part of it.
Privacy and Anonymity	Unlinkability of anonymous communications	Sender	• A sender shall not be linked to its sent message to prevent attackers from learning of the message's origin.
		Receiver	• A receiver shall not be linked to the received message to prevent attackers from learning of the message's destination.
		Sender–receiver	• The sender and receiver shall not be linked together to prevent attackers from learning of the sending and receiving ends. They are also relatively anonymous to each other.
	Type of management	Centralized	• A system relays messages through a trusted anonymous entity to hide identities of the sender and receiver.
		Distributed	• A system relays messages through a group of anonymous entities to hide the identities by various means such as encapsulating messages.
Secure routing	Management		• A system can establish and maintain routing-related information in a centralized or distributed manner.
	Prevention		• Updating routing information (e.g., a membership status and routing paths) must be restricted to authorized members. • A new routing path should be tested such that any routing black hole and loop are entirely eliminated.

Table 3. *Characteristic of security services in SGC over wireless networks.*

eral means, including hashing and signing the message along with strong encryption keys. In ad hoc networks, group members may have different capabilities and protocols to perform different levels of encryption on group messages. Thus, some messages may be encrypted with strong encryption, while others with weak encryption are relatively easily breakable. In WSNs sensor nodes may have similar capabilities and protocols that are embedded before deployment. Confidentiality ensures that only authorized members can retrieve meaningful data from the message.

Group survivability and availability: An attacker can attack routing hosts (i.e., access points and base stations) to isolate some or all group members, or partition the group. Thus, all routing hosts must be protected 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. Group availability ensures that only authorized users can always communicate within the group by using restricted group resources, and any violation exceeding the limitation of group resources will be promptly detected.

Table 2 illustrates each discussed attack along with security services that can be deployed to mitigate its impact. For example, the impact of a flooding attack may be partially mitigated by authenticating sources that generate flooding packets along with early detection of a massive amount of packets originated by a single source. Thus, flooding packets would be dropped immediately once such an attack has been detected. Unauthorized routing update can be detected and prevented by the following services: authenticating both source and message to determine

The security analysis shows that MOMBASA is protected against various attacks by using three security components: packet filtering at access network boundaries, deployment of an authentication, authorization, access control (AAA) infrastructure, and rate limiting against DoS attacks.

whether the routing update message is legitimate and originated by an authorized member; enforcing access control over a routing table; signing the routing update message such that message integrity is preserved and no attacker has falsely modified the message; encrypting all management packets (routing update requests and replies); and any loophole or sinkhole routing, which possibly leads to a denial of service, will be tested, detected, and fixed prior to actual deployment.

SGC over Wireless Infrastructure Networks

This section surveys some SGCs that provide security protection over wireless infrastructure networks.

DeCleene *et al.* [5] presented a hierarchy-based key management protocol that divides an operational field into administratively independent areas. The area key is used to encrypt the message containing the data key. The data key is a network-wide shared key, and is used to encrypt the data message. When users frequently move within areas, the area key is rekeyed, thereby resulting in significant degradation of group performance in terms of processing and communication overheads. Thus, several rekeying algorithms have been proposed to reduce the need for rekeying, thus decreasing communication and processing overheads. The delayed rekeying algorithm uses the extra key owner list (EKOL) to store the area keys belonging to the leaving member and that member's ID. When that member re-enters the area, the area keys are restored. However, once the EKOL is full, the first recorded area keys are discarded to make room for other members. A member can only hold a limited number of area keys.

Pros: Low overheads; highly dynamic membership is supported.

Cons: The area keys may be compromised easily since the area keys have been repeatedly reused for often moving members.

Sun *et al.* [12] matched tree-based key management with the physical cellular network topology in order to build a topology-matching key management (TMKM) tree. When the user moves among cells, an efficient handoff mechanism handles the relocation of that user in the TMKM tree. Each cell has a corresponding wait-to-be-removed (WTB) list that keeps track of previous and current cell members. A relocation of a member between two cells requires a rekeying process to preserve the key secrecy. The rekeying process is performed based on information from the WTB lists of these cells. The key manager, called the key distribution center (KDC), maintains and updates the WTB lists of all cells in the network accordingly. The communication overheads incurred by the rekeying process can be reduced by delivering new keys locally in the TMKM tree only to members who need the rekeyed keys. It was shown that communication overheads due to the efficient handoff rekeying processes using the TMKM tree scheme can be reduced as much as 80 percent compared to those using conventional topology independent key management (TIKM) tree schemes.

Pros: Low communication overheads.

Cons: The scheme does not consider the overheads incurred by the KDC that could result in very poor performance in the actual deployment.

Gupta and Cherukuri [1] presented three schemes: single session key (SSK), different session key (DSK), and a combination (HYBRID). These schemes are based on location-based access control in which only users who are located in specific locations can access the services. In the SSK scheme, a base station (BS) assigns the same session key (sk) to all members. In the DSK scheme, a BS assigns a different session key to each member. In the HYBRID scheme, a BS assigns the same sk to all members who have been *stable* in the cell for more than a specified period of time; otherwise, it assigns a different sk to a *nonstable* member.

Pros: Their simulations of SGC over all cellular networks with high mobility showed that the communication overhead using the HYBRID scheme is lower than that using the DSK and SSK schemes.

Cons: Strict time synchronization is required to determine whether a member is classified as stable or nonstable; the scheme did not provide a means for base stations to exchange information on their members; and handoffs, which can incur more overheads, were not addressed.

Westerhoff *et al.* [13] presented a decentralized architecture called mobility support — a multicast-based approach (MOMBASA) to achieve low latency for handoffs with minimum packet loss as well as secure protocol operations. MOMBASA enables each mobile node to register with a proxy, called a Mobility-Enabling Proxy (MEP), which in turn participates in the multicast group on behalf of the mobile node. The mobile node communicates with the MEP via unicast, while the MEP communicates with the multicast group via multicast. Thus, the MEP converts unicast and multicast packets between the mobile node and the multicast group. Security analysis shows that MOMBASA is protected against various attacks by using three security components: packet filtering at access network boundaries, deployment of an authentication, authorization, and access (AAA) infrastructure, and rate limiting against DoS attacks.

Pros: MOMBASA is provably secure from many threats; performance degradation due to handoffs is negligible (low-latency handoff); less packet loss; and the workloads among access points and the AAA server are fairly distributed.

Cons: The scheme only considers handoffs when the MEP is no longer functioning, but not the case when the membership is highly dynamic. When there are messages destined for idle nodes, the MEP associated with these nodes has to multicast the paging update messages to other MEPs, thus incurring a significant overhead.

SGC over Mobile Ad Hoc Networks

This section surveys some SGCs that provide security protection specifically over mobile ad hoc networks.

Kaya *et al.* [11] proposed a dynamic multicast group management protocol that attempts to equally distribute the workload of securing communications to all participating members. Group information and associated security services are disseminated and maintained by all members throughout MANETs, and service rights certificates are given by the designated group manager to members for accessing information. The group manager is temporarily selected per session, and it establishes a physical security tree, authenticates prospective members, updates the security tree per membership change, and handles the revocation of certificates. The security tree is used to securely forward the shared group key to members, while the data multicast tree is used to forward the encrypted data messages to authorized members.

Pros: Communication overheads and latency of joining/leaving/key revocation processes do not substantially degrade the group performance as the number and speed of joining/leaving nodes increase.

Cons: 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. The simulation tried to illustrate the impact of dynamic membership with a very small number of nodes, and the results may not be valid for a large group.

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: 2^d-Octopus and Tree-Based Group Diffie-Hellman (TGDH)-based 2^d-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 MANETs.

Pros: The modified Merkle tree-based scheme with TGDH-based 2^d-Octopus has lower communication and processing overheads than that with 2^d-Octopus and another existing protocol, one-way function tree (OFT), as the size of the group increases.

Cons: The scheme did not discuss how this integration of authentication and key distribution could better protect SGC against various threats, such as DoS and collusion attacks.

Balachandran *et al.* [10] proposed a key agreement scheme for SGC over MANETs, referred to as the Chinese Remainder Theorem and Diffie-Hellman (CRDTH) scheme, which aims 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 mutually generate the group key based on the Chinese remainder theorem (CRT).

Pros: The scheme can equally distribute the computational workloads to all members. The scheme requires 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. No a priori knowledge and member serialization are required. Highly dynamic membership is supported.

Cons: The authors only suggested how the scheme would be compromised rather than validating the security of the scheme.

Lazos and Poovendran [14] presented the routing-aware key distribution (RAwKey) problem and proposed an optimal solution that minimizes energy expenditure caused by the rekeying process in an energy-constrained wireless ad hoc network. The key idea is to construct an energy-efficient key distribution scheme (operating at the application layer) for SGCs over ad hoc networks by gathering cross-layer information from the physical layer (i.e., the node transmission power) and the network layer (i.e., the multicast routing tree).

Pros: The performance of the optimal energy-efficient solution for rekeying does not substantially change as the group size varies, and the cross-layer algorithm can obtain a suboptimal solution with low complexity.

Cons: The complexity of the scheme is still rather high, and the efficiency for actual deployment remains a great challenge.

SGC over Wireless Sensor Networks

This section covers SGCs that provide security protection over WSNs.

Zhu *et al.* [6] proposed a key management protocol, called a localized encryption and authentication protocol (LEAP), for large-scale distributed sensor networks. The protocol is designed based on two observations: different packet types exchanged among sensor nodes require different security services, and a single key management scheme may not be suitable for various security requirements. The proposed scheme uses four types of keys for fundamental security services (e.g., authentication and access control) to secure communications. These four types of keys include a pair-wise key used between a sensor node and the base station, a pair-wise key used between a pair of two sensor nodes, a shared cluster key used among all sensor nodes in the same cluster, and the group key used among all sensor nodes. Thereafter, the scheme provides security services that can mitigate several attacks. For example, authentication of one-hop broadcast communications among nodes with one-way key chains can mitigate the impersonation attack, and a timestamp is used to expire keys to prevent node capture and sybil attacks.

Pros: Low communication overheads; the scheme is energy efficient.

Con: The scheme did not discuss the power consumption of sensor nodes in deploying some of the proposed security mechanisms.

Yu and Guan [7] proposed a group-based key predistribution 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 in such a way that the number of neighbors of a node is minimized, thereby reducing power consumption. The scheme classifies communications of sensor

The LEAP protocol is designed based on two observations: different packet types exchanged among sensor nodes require different security services, and a single key management scheme may not be suitable for various security requirements.

The B-PCGR scheme has two limitations: an attacker can retrieve the polynomials by searching only 1-hop away neighboring nodes of the victim, and to successfully stage an attack requires compromising only a small number of 1-hop neighboring nodes.

nodes into two types: intergroup and in-group. The secret matrix G is shared by all groups, and each group is distinctively assigned a secret matrix A. Each node selects correspondingly a column from matrix G and a row from matrix A. Thus, two nodes in the same group can compute the pair-wise key used to secure in-group communications. Furthermore, a number of secret B matrices are selectively assigned to groups in such a way that any two neighboring groups share a portion of the secret matrices. Then the two neighboring groups determine which of the shared secret B matrices they share in order to generate the shared keys. Upon key generation, two nodes in neighboring groups mutually agree on which rows will be selected from these previously selected B matrices. Thus, they can compute the pair-wise key used to secure intergroup communications.

Pros: 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. Furthermore, the connected components define a graph in which any two nodes can always find a route between them. The scheme incurs low storage overhead, and offers a better safeguard against node capture attacks than several existing schemes.

Cons: 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. The computational and time complexities might be substantial.

Zhang and Cao [8] proposed a set of predistributed and local collaboration-based group rekeying (PCGR) schemes to mitigate the node capture attack and the DoSS attack. The basic-PCGR (B-PCGR) scheme was first proposed with the assumption that the future group keys can be preloaded into the sensor nodes before deployment. Thus, the future keys must be protected by encryption with some polynomials, which are kept by some one-hop neighboring nodes. Thus, the B-PCGR scheme requires all sensor nodes to collaborate with each other to retrieve their encrypted future keys, and detect and protect themselves against any attempt to compromise nodes. However, the B-PCGR scheme has two limitations: an attacker can retrieve the polynomials by searching only one-hop neighbor nodes of the victim, and to successfully stage an attack requires compromising only a small number of one-hop neighbor nodes. To overcome the first limitation, the cascading PCGR (C-PCGR) scheme is proposed to distribute the polynomial shares to two- or three-hop neighboring nodes. To overcome the second limitation, the random-variance-based PCGR (RV-PCGR) scheme is proposed to add *random variance* numbers to the polynomials to strengthen the polynomials in order to make it more difficult for the attacker to retrieve the encrypted future keys.

Pros: The schemes can effectively protect SGC against node capture and DoSS attacks.

Cons: Rekeying is very limited due to a limited number of reusable future keys. A priori knowledge of group operations (e.g., a set of future keys, a key generating function, and group joining/leaving processes) is required, and thus any real-time adaptation of these group operations cannot be performed online. The collaboration of nodes is required, but in many sensor networks such collaboration may not be possible at all and also may cause unnecessary power consumption.

Huang *et al.* [15] 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 an intrusion detection and deletion mechanism. The SLIMCAST protocol divides a group routing tree into levels and branches in a clustered 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. SLIMCAST enables an upstream node to aggregate data packets from its downstream children nodes, and then re-encrypts the aggregated packet with the level keys this node shares with its parent nodes. The re-encrypted packet is then sent upstream toward a base station. Furthermore, duplicate packets from the sibling nodes will be discarded to reduce redundant bandwidth and power consumption.

Pros: Low communication overheads and power consumption. Performance does not substantially degrade as the group size increases.

Cons: The performance is degraded (i.e., high power consumption) when membership changes are massive.

Wadaa *et al.* [2] proposed an energy-efficient protocol to provision anonymity in WSNs. The protocol divides the network into clusters. Two activities are defined in each cluster: intracluster activity (i.e., data generation) and intercluster activity (i.e., data transmission). For intracluster activities inside a cluster, a node periodically collects and formulates the sensor readings, and then reports to the designated entity, called the transaction instance manager. The manager collects all node reports and formulates the transaction instance report (TIR). For intercluster activities, all managers send the TIR to the sink node (i.e., a base station) through neighboring managers in a hop-by-hop manner. Then the protocol formulates the anonymity problem, and identifies and eliminates the minimum number of nodes that cause the maximum loss of sensor readings.

Pros: Energy-efficient. Performance does not substantially degrade as the group size increases.

Cons: The scheme did not analyze or prove substantially the anonymity level per transmission.

Karlof and Wagner [3] discussed attacks that can disrupt group routing in WSNs. The survey article illustrates how each attack is executed, and describes the existing mechanisms in mitigating the attacks.

Note that SGCs proposed for the above three types of networks may be adapted to other types of wireless networks, but consideration of such adaptation is beyond the scope of this article.

Schemes Characteristics	Wireless infrastructure networks				Mobile ad hoc networks				Wireless sensor networks				
	[5]	[12]	[1]	[13]	[11]	[9]	[10]	[14]	[6]	[7]	[8]	[15]	[2]
Key management	Hierarchical-based	Topology-matching tree	Area-based and batch rekeying	N/A[1]	Ad hoc group key (AGK)	Tree-based group Diffie-Hellman (TGDH)	Chinese remainder and Diffie-Hellman	Routing-aware key distribution	Cluster-based keys	Group-based key	Locally group-based key and key predistribution	Cluster-based tree (level and branch)	N/A
Authentication	N/A	N/A	User auth.	Key and message auth.	Certificate-based PK[2] 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
Authorization/ access control	N/A	N/A	Location-based	Packet filtering	Certificate	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Accounting/ nonrepudiation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes	N/A
Message integrity and confidentiality	Yes	N/A	Yes	Yes	Yes	Yes	Yes	Yes	N/A	N/A	N/A	Yes	N/A
Privacy/ anonymity	N/A	N/A	Privacy of user's location	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes (virtual infrastructure)
Survivability/ availability	N/A	N/A	N/A	N/A	Yes (quick recovery)	Yes	N/A	N/A	Yes	Yes	Yes	N/A	Yes
Attack prevention[3]	N/A	N/A	Eavesdropping	DoS, identity, replay, source address spoofing	Message modification, replay	Impersonate, collusion	N/A	N/A	Wormhole, sinkhole, Sybil, DoS, replay, insider	Node capture	Node capture, eavesdropping, DoSS	Node capture, Sybil	DoS, traffic analysis
Reducing communication overheads	Yes	Yes (using locality to reduce comm. complexity)	Yes (with HYBRID scheme)	N/A	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	Yes	Yes	Yes (with HYBRID scheme)	N/A	N/A	Yes	Yes	N/A	Yes	N/A	Yes	Yes	N/A
Handling high mobility	Yes	Yes	Yes	Yes	Yes	N/A	Yes	Yes	N/A	N/A	N/A	Yes	N/A
Handling handoffs	Yes (but needs back channels)	Yes	N/A	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Steady performance vs. group size	N/A	Yes	N/A	N/A	Yes	Yes	N/A	Yes	N/A	N/A	N/A	Yes	N/A
Scalable	Yes	Yes	N/A	N/A	Yes	Yes	Yes	Yes	N/A	N/A	N/A	Yes	Yes
Energy-efficient	N/A	N/A	N/A	N/A	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 4. *Comparison of SGC over wireless networks.*

Open Challenges

Here, we outline some challenges that should be tackled, and define future research directions on SGC over wireless networks.

Integration of security services. As illustrated in Table 2, most attacks can be greatly mitigated by the fundamental security services. Thus, it is still the greatest challenge to design an energy-efficient scheme that integrates more security services to satisfy various security requirements, particularly authentication, access control, and nonrepudiation (via group signatures), without incurring significant overheads.

Deployment of SGC in heterogeneous wireless networks. With higher demand for more

The number of applications of group communications over wireless networks has been steadily increasing However, communications over wireless channels is insecure and easily susceptible to various kinds of attacks.

functionalities in wireless devices, an SGC scheme should be able to be deployed in heterogeneous wireless networks, including cellular networks, wireless LANs, wireless ad hoc networks, and WSNs, and support communications over a hybrid of wireless and wired networks.

Optimization of group performance with respect to overheads and limited resources. To be efficient, a scheme should optimize group performance subject to overheads (communication, processing, and storage) and limited resources (memory, bandwidth, and power supply).

Extension to IPv6 wireless networks. An IPv6 wireless network seems to be a promising next-generation network, and some work is addressing end-to-end built-in security. Future research on SGC is engineered to support IPv6 wireless networks.

CONCLUSIONS

The number of applications of group communications over wireless networks has been steadily increasing, such as group-oriented military systems (in-the-field commander conference over wireless devices) and education systems (teacher lectures in a distance learning classroom). However, communications over wireless channels is, by nature, insecure and easily susceptible to various kinds of attacks. Much existing work has attempted to incorporate security into such communications.

To better understand SGC over wireless networks, we have presented known attacks that can severely disrupt or even shut down group communications in wireless networks. The we have discussed necessary security requirements, and illustrated fundamental security services to meet these requirements and safeguard the communications against these attacks. We have demonstrated that several attacks can be prevented and mitigated by the proposed security services. We have also reported several existing works on SGC over three types of wireless networks: wireless infrastructure networks, mobile ad hoc networks, and wireless sensor networks, as summarized in Table 4. 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. To complete the survey on SGC over wireless networks, we have presented some open challenges that still need to be overcome.

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 ssuel 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] Y. Sun, W. Trappe, and K. J. Ray Liu, "A Scalable Multicast Key Management Scheme for Heterogeneous Wireless Networks," *IEEE/ACM Trans. Net.*, vol. 12, no. 4, Aug. 2004, pp. 653–66.

[13] L. Westerhoff *et al.*, "Security Analysis and Concept for the Multicast-Based Handover Support Architecture MOMBASA," *Proc. IEEE GLOBECOM 2004*, vol. 4, Dec. 2004, pp. 2201–07.

[14] 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.

[15] 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.

BIOGRAPHIES

PITIPATANA SAKARINDR (ps6@njit.edu) received a B.E degree from King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand, in 1999, and an M.S. degree in computer engineering from the New Jersey Institute of Technology (NJIT), Newark, in 2002. He is currently pursuing a Ph.D. in electrical eengineering at NJIT. His current research focuses on various aspects of network security, including security-integrated quality of service, trust and reputation models, anonymous networks, and cryptography.

NIRWAN ANSARI (nirwan.ansari@njit.edu) received a B.S.E.E. (summa cum laude) from NJIT in 1982, an M.S.E.E. degree from the University of Michigan, Ann Arbor, in 1983, and a Ph.D. degree from Purdue University, West Lafayette, Indiana, in 1988. He joined NJIT's Department of Electrical and Computer Engineering as an assistant professor in 1988, and has been a full professor since 1997. He has also assumed various administrative positions including the Newark College of Engineering's Associate Dean for Research and Graduate Studies at NJIT. He authored *Computational Intelligence for Optimization* (Springer, 1997, translated into Chinese in 2000) with E. S. H. Hou, and edited *Neural Networks in Telecommunications* (Springer, 1994) with B. Yuhas. His current research focuses on various aspects of broadband networks and multimedia communications. He has also contributed approximately 300 technical papers including over 100 refereed journal/magazine articles. He is a Senior Technical Editor of *IEEE Communications Magazine*, and also serves on the editorial board of *Computer Communications*, *ETRI Journal*, and *Journal of Computing and Information Technology*. He was the founding general chair of the First IEEE International Conference on Information Technology: Research and Education; was instrumental, while serving as its Chapter Chair, in rejuvenating the North Jersey Chapter of the IEEE Communications Societ,y which received the 1996 Chapter of the Year Award and a 2003 Chapter Achievement Award; served as Chair of the IEEE North Jersey Section and in the IEEE Region 1 Board of Governors during 2001–2002; and has served on various IEEE committees.