ISSN 2319 – 7757 EISSN 2319 –7765

Indian Journal of

Engineering

Security threads and quality of service challenges for wireless sensor networks: A Survey

Mallikarjun Talwar[1], Mallikarjun C Sarasamba[2]

1.Asst.Prof Electronics and Communication Dept BKIT Bhalki,Bidar,India e-mail: talwar.mallu@gmail.com
2.Asst.Prof Electronics and Communication Dept BKIT Bhalki,Bidar,India e-mail: mallikarjun.Sarasamba@gmail.com

Publication History
Received: 25 January 2014
Accepted: 14 March 2014
Published: 2 April 2014

Citation
Mallikarjun Talwar, Mallikarjun C Sarasamba. Security threads and quality of service challenges for wireless sensor networks: A Survey. *Indian Journal of Engineering*, 2014, 10(21), 15-23

ABSTRACT

Security and quality of service (QoS) issues in cluster-based wireless sensornetworks are investigated. The QoS perspective is mostly at application levelconsisting of four attributes, which are spatial resolution, coverage, and system lifetime and packet loss due to collisions. The addressed security aspects aremessage integrity and authentication. Under this scope, the interactions betweensecurity and service quality are analyzed with particular emphasis on the tradeoffbetween security and spatial resolution for channel capacity. The optimal securityand spatial resolution levels which yield the best tradeoff are determined.In addition, a control strategy is proposed to achieve the desired quality of service and security levels during the entire operation of a cluster-based sensor network.

Keywords: Wireless sensor networks, security, quality of service, spatial resolution, coverageIntroduction

1. INTRODUCTION

Wireless sensor networks (WSN) provide efficient and reliable means for the observation of some physical phenomena which are otherwise very difficult, if not impossible, to observe, and initiation of right actions based on the collectiveinformation received from sensor nodes (Akyildiz et al., 2002). This feature of WSN has significant impact on several military and civil applications such as disaster management, field surveillance and environmental monitoring (Kuorilehto et al., 2005). Due to strict energy limitations of sensor nodes and their deployment in large numbers, most of the research efforts on WSN focused on communication protocols. These are usually required to be energy aware to maximize network lifetime and scalable to accommodate large quantities of sensors (Shah and Rabaey, 2005). Besides, because medium access is a major consumer of sensor energy, energy-efficient medium

access control (MAC) mechanisms are also explored. The common feature of these research works is that they address the communication problems of WSNapplications that require conventional data communications where main concernis energy-efficiency but they do not consider service quality requirements of sensor networks. However, the envisioned WSN applications introduce quality of service (QoS) requirements for sensor networks of near future. For instance, real-time WSN applications such as target tracking call for bounded delay and guaranteed bandwidth. Similarly, surveillance applications like habitat monitoring require a certain level of data precision, a pre-defined coverage guarantee and maximal monitoring time. Therefore, those service quality requirements for WSN span a wide category of attributes ranging from network QoS including latency, jitter, and throughput and packet loss to application QoS composed of spatial resolution, coverage, and exposure and system lifetime. For envisioned sensor network applications of near future, another requirement, which is also as important as QoS, is an effective security mechanism. Since sensor networks may be in interaction with sensitive data or operate in hostile unattended environments like battlefields, protection of sensor data from adversaries is an inevitable requirement. Similarly, for commercial applications of WSN, the protection of privacy such as personal physiological and psychological information is equally important. QoS and security mentioned in the previous two paragraphs are not uncorrelated issues in the context of sensor networks, and hence, it is important to consider them together. The reason is two-fold. First, there are such WSN settings where both QoS and security are required for successful operation of the sensor network. one example of which is a military target tracking application (Figure 1). The second reason is the considerable amount of interactions between these two concepts .In other words, adding security to a protocol impacts the level of QoS that can be provided, and similarly, choice of QoS mechanisms might affect the security level of the network. Therefore, thereare both positive and negative impacts of security on QoS and vice versa and, QoS and security are not orthogonal concepts but have remarkable correlations. Thus, providing both security and QoS for sensor networks in a joint fashion is achallenging task not only due to the limited resources of WSN but also due to the complex interactions between the two. Still, however, this challenge should be taken because of the potential near-future WSN applications which require secure and QoS-provisioned transmission of data.

2. QOS CHALLENGES IN SENSOR NETWORKS

The unique characteristics and requirements of sensor networks pose newchallenges for QoS support in WSN in addition to the ones inherited from generalwireless networks such as link quality and dynamic network environment. Some of these sensor network QoS challenges cited in the literature (Chen et al., 2004). Such as bandwidth constraints, resource limitations, energy-delay tradeoff, data redundancy, multiple traffic types, unbalanced traffic, scalability, multiple sinks, network dynamics, energy.

Bandwidth constraints: Real-time multimedia applicationshave high bandwidthrequirements that is hard to satisfy even on wire-based networks. Sensornetworks, however, have very scarce bandwidth available to them. Furthermore, sensor nodes not only relay their own data but also relay the packets coming from other nodes due to multihop communication strategy and thisputs more burden on the available bandwidth. In addition, traffic in a sensor network can be composed of a mix of real-time and non-real-time traffic. Dedication of whole bandwidth to real-time data requiring QoS is not acceptable and a tradeoff in multimedia data quality might be needed to accommodate non-real-time traffic. A solution toovercome those bandwidth limitations might be use of ultra wideband (UWB) technologies.

Resource limitations: Wireless sensor networks have very stringent constraints on resources such as energy, memory, processing capability, and transmission power and buffer size. Most important of these limitations is available energy of nodes because it is not feasible to replace or recharge the batteries of sensors once deployed in the field and depletion of energy of a node renders it unusable. Consequently, QoS support mechanisms for WSN should be designed in simplicity and low-complexity avoiding computation intensive algorithms, expensive signaling protocols and overwhelming state information on nodes which increases power consumption. Energy-Delay tradeoff: Because the transmission power of sensor node radios is limited, use of multi-hop routing is the most common technique in WSN data communication. Although use of multi-hop routing decreases energy consumption of individual nodes during transmission, it comes with a cost, that is, increased latency in end-to-end packet transfer. This increase in accumulated delay is mostly due to packet queuing (not propagation delay) at multiple sensor nodes and therefore it complicates the analysis and handling of QoS constrained traffic. Thus, it may be unavoidable to sacrifice energy efficiency to meet timely delivery requirements when designing QoS methods for sensor networks.

Data redundancy: High redundancy in the generated data is a characteristic of wireless sensor networks. For conventional unconstrained traffic, using aggregation functions to eliminate redundant data is helpful. However, data fusion or aggregation for QoS constrained multimedia traffic is not a trivial task. Comparing video streams or images is a computationally expensive task and consumes energy resources. In addition, these complex computations may also increase latency and therefore complicates QoS design in WSN further. Using a combination of system and sensor

Mallikarjun Talwar et al.
Security threads and quality of service challenges for wireless sensor networks: A Survey,
Indian journal of engineering, 2014, 10(21), 15-23,

level rules might be a solution to make aggregation of QoS traffic computationally feasible. For example, aggregation of imaging data can be selectively performed for data generated by sensor nodes pointing to very close directions.

Multiple traffic types: Since sensor networks usually include heterogeneous sets of sensors, several issues arise regarding support of QoS constrained traffic. For instance, some WSN applications require a mixture of sensor nodes for temperature, pressure and humidity monitoring of the surrounding environment, motion detection using acoustic signatures and capturing image or video of moving targets. Reading of generated data from these sensors can be at different rates, subject to diverse quality of service constraints and following multiple data delivery models. So, this kind of a heterogeneous environment makes QoSsupport more challenging. Unbalanced traffic: In majority of sensor network settings, traffic flow is from a large number of sensor nodes to a small set of sink nodes. Therefore, this unbalanced traffic should be taken into account when designing QoS mechanisms for wireless sensor networks.

Scalability: A usual sensor network is composed of hundreds or even thousands of individual sensor nodes densely deployed in the environment. Therefore, QoS schemes designed for WSN should be able to scale up to an enormous number of nodes. For instance, provided QoS should not degrade quickly when deployed node density increases.

Multiple sinks: In a sensor network, there may exist more than one sink node, which impose different requirements on the network. For example, one sink may ask sensor nodes located in the southeast of the sensor field to send a temperature report every one minute, while another sink node may only be interested in an exceptionally high temperature event in the northwest area. WSNs should be able to support different QoS levels associated with different sinks.

Network dynamics: Network dynamics may arise from node failures, wireless link failures, node mobility, and node state transitions due to the use of power management or energy efficient schemes. Such a highly dynamic network greatly increases the complexity of QoS support. Energy balance: In order to achieve a long-lived network, energy load must be evenly distributed among all sensor nodes so that the energy at a single sensor node or a small set of sensor nodes will not be drained out very soon. QoS support should take this factor into account.

Packet criticality: The content of data or high-level description reflects the criticality of the real physical phenomena and is thereby of different criticality or priority with respect to the quality of the applications. QoS mechanisms may be required to differentiate packet importance and set up a priority structure.

3. SECURITY REQUIREMENTS OF SENSOR NETWORK APPLICATIONS

The fundamental security requirements for typical data networks are confidentiality, integrity and availability, which are also known as CIA triad. These are accompanied by other requirements such as authentication, nonrepudiation, Accountability, etc. Sensor networks share most of these requirements but also pose unique requirements of their own. These security requirements for sensor networks are data confidentiality, data integrity, data freshness, authentication and availability as given in (Walters et al., 2006).

Data confidentiality: In the context of sensor networks, confidentiality relates to the following: (1) Sensor nodes in a sensor network should not leak sensor readings to non-participating parties. Particularly in military applications, data stored in sensor nodes may be highly sensitive. (2) In many applications, nodes communicate confidential data such as key distribution. Therefore, it is very important to build a secure channel in a wireless sensor network. (3) Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

Data integrity: Providing confidentiality prevents disclosure of data to an adversary. However, this doesn't mean that data is fully safe. The adversary can change the data, with the aim of putting the sensor network into confusion. For instance, a malicious sensor node may add some fragments or modify the data within a packet. This new packet can then be sent to the original receiver leading it into error. Data integrity can be spoiled due to the harsh communication environment even without the presence of a malicious node. Therefore, data integrity providing schemes should be used in WSN to ensure any received data has not been altered in transit. Data freshness: Even if confidentiality and integrity of data are assured, it is also needed to ensure the freshness of each message since sensor networks stream some forms of time-varying measurements. Data freshness implies that the data is recent, and it ensures that no old messages have been replayed. This requirement is particularly important when shared-key strategies are employed in the design. Shared keys need to be changed over time and it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack and to disrupt the normal work of the sensor, especially if the sensor is unaware of the new key change time. To solve this problem, a nonce or another time-related counter can be added into the packet to ensure data freshness.

Authentication: Authentication allows a receiver to verify that the data really is sent by the claimed sender. It is important for several applications in sensor networks. For example, authentication is necessary for many administrative tasks such as network reprogramming or controlling sensor node duty cycle. In addition, a malicious node can easily inject messages, so the receiver needs to ensure that the data used in any decision-making process comes from the correct source. In the two-party communication case, data authentication can be achieved through a

Mallikarjun Talwar et al.
Security threads and quality of service challenges for wireless sensor networks: A Survey,
Indian journal of engineering, 2014, 10(21), 15-23,

symmetric key mechanism: The sender and the receiver share a common secret key to compute a message integrity code (MIC) which is appended to the data payload. When a message with a correct MIC arrives, the receiver knows that it must have been sent by the sender. This kind of authentication cannot be applied to a broadcast setting unless much stronger trust assumptions are placed on the network nodes. If one sender wants to send authentic data to mutually mistrusted receivers, use of a symmetric MIC is insecure: Any one of the receivers knows the MIC key, and hence could impersonate the sender and forge messages to other receivers. Hence, asymmetric mechanisms are needed to achieve authenticated broadcast.

Availability: Availability refers to the readiness of data for the access of the authorized users when needed. Denial of service (DoS) attacks, which are the most common threat for the availability of traditional networks, threaten also the availability of sensor networks. Most common form of DoS attack are in the form of jamming where an adversary attempts to disrupt the operation of WSN by broadcasting a high energy signal. Or, attackers can induce battery exhaustion in sensor nodes by sending a sustained series of useless communications that the targeted nodes will expend energy processing. Thus, security protocols designed for sensor networks should protect against attacks which menace the availability of the network.

4. SECURITY CHALLENGES IN SENSOR NETWORKS

Conventional communication networks, the security mechanisms utilized to support the CIA triad is well known and have been in use for years. For instance, Symmetric key encryption algorithms such as DES, 3DES, AES, RC4, etc. and public key encryption algorithms such as RSA, Elliptic Curve, Knapsack, etc. are in use to provide confidentiality. In order to provide authentication and integrity, message integrity codes, digital signatures, one-way hash functions, etc. are utilized. However, due to the unique challenges posed by sensor networks, traditional security techniques cannot be directly applied to WSN. Challenges in WSN security design can be classified into four broad categories, which are resource constraints, unattended operation, in-network processing and unreliable Communication. These WSN security challenges are briefly explained in the following (Walters et al., 2006).

Resource constraints: All security approaches require a certain amount of resources to be implemented such as memory, computational power and energy. However, developed to be compact, sensor nodes are very limited in terms of storage capacity, processing capability and energy sources. For instance, a common sensor type has a 8-bit 4MHz processor with a total of 8K memory and disk space. With such a limitation, the size of the security software developed for a sensor should also be quite small. Besides, it is not feasible to performcomputationally complex security algorithms like public key cryptography using very incapable processors of sensor nodes. In a similar way, the limited power capacity of sensors and the inability to replace and recharge batteries once depleted puts strict limitations on the use of energy. Therefore, energy impacts of proposed security schemes for WSN should also be taken into account. Because cryptographic methods cause extra power consumption due toprocessing functions such as encryption, decryption, verification etc. and also due to transmission of cryptographic overhead like digital signatures, energy efficientsecurity algorithms should be designed for sensor networks.Unattended operation: Though it depends on the function of the particular sensor network, sensor nodes may be left unattended for long periods of time. There are three main caveats to unattended sensor nodes: (1) Exposure to physical attacks: Sensors may be deployed in an environment open to adversaries, harsh physicalconditions, bad weather, and so on. The possibility of a sensor to suffer a physicalattack in such an environment is much higher than a typical network computer, which is located in a secure place and mainly faces attacks from a network.Therefore; attackers may capture sensor nodes, extract cryptographic keys, modifyprogramming codes, or even replace them with malicious nodes under attacker's control. As a result, the challenge is to build secure networks which can operatecorrectly even when many nodes have been compromised and behave in amalicious way (2) Maintenance difficulties: Since sensor networks usually operate in areas which are far from the control point, it is almost impossible to detectphysical tampering (i.e., through tamper-proof seals) and deal with physicalmaintenance issues (e.g., battery replacement). An example of such a case is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed. Thus, security mechanisms used for WSN should not require any maintenance (3) Lack of central management: A sensor network is a distributed network without a central management point. Although this increases the vitality of the sensor network, it requires that distributed security schemes be used for WSN security. In-network processing: Mostly, the dominant traffic pattern in sensor networks is many-to-one, with many sensor nodes communicating sensor readings or network events back to a central base station. In-network processing such as aggregation, duplicate elimination, or data compression is used to make this communication pattern in an energy efficient manner. Since in-network processing requires intermediate nodes to access, modify, and possibly suppress the contents of messages, it is highly unlikely that end-to-end security mechanisms between a sensor node and a base station can be used to guarantee integrity, authenticity, and confidentiality of such messages. Instead, link layer security mechanisms can be used.

Mallikarjun Talwar et al.
Security threads and quality of service challenges for wireless sensor networks: A Survey,
Indian journal of engineering, 2014, 10(21), 15-23,

Table 1
Layer attacks against sensor networks routes, generate false error messages, partition the network, increase end-to-end latency, etc.

Threats	Description
Selective forwarding	Malicious node blocks the passage of all or selective messages
Wormholes	Two malicious nodes in different parts of the network colluding to understate their distance from each other to deceive other nodes.
Sybil	Malicious node illegally claims multiple identities
Sinkhole	Fool large number of nodes that compromised node has the high quality route.
Hello Floods	Malicious node with larger enough transmission power, flood Hello packets to far nodes to deceive them to use false route, to cause confusion to the networks.
Acknowledgement spoofing	Spoof Acknowledgement message to sender with reverse information
Cloning	Malicious node clones the requests, thus inducing an Alternative data flow to itself.

Unreliable communication: The poor quality of wireless channel causes high transmission error rates and more packet loss in sensor networks. If the communication protocol used lacks appropriate error handling, critical security packets like cryptographic keys can be lost. Even if the channel is sufficiently reliable, collisions may occur due to the broadcast nature of wireless sensor networks causing critical packet losses. In addition, multi-hop routing, network congestion and processing at nodes may lead to latency in the network and it may be difficult to achieve synchronization among nodes. This synchronization problem can be critical to sensor network security where security mechanism relies on key distribution.

5. ATTACKS AGAINST SENSOR NETWORKS

Since they are deployed usually in unprotected areas where several security threats exist, sensor networks are vulnerable to several kinds of attacks. These attacks can be performed in a variety of ways ranging from denial of service attacks to physical attacks. Main attack types that can be launched against Wireless sensor networks are covered in this subsection.

DoS Attacks: A DoS attack is "any event that diminishes or eliminates a network's capacity to perform its expected function (Wood & Stankovic, 2002). DoS attacks on sensor networks range from simple jamming of sensor'scommunication channel to more sophisticated attacks violating 802.11 MAC protocol or any other layer of the protocol stack. DoS attacks can be very dangerous when sensor networks are used in highly critical and sensitive applications. For instance, a sensor network designed to alert building occupants in the event of a fire could be highly susceptible to a denial of service attack. Even worse, such an attack could result in the deaths of building occupants due to the non-operational fire detection network. Another possible use for wireless sensors is the monitoring of traffic flows which may include the control of traffic lights. A denial of service attack on such a sensor network could be very costly.

Attacks against privacy: Since sensor networks provide increased data collection capabilities, threats against privacy of collected data are a relevant concern for WSN. Adversaries may use even seemingly insensitive data to derive sensitive information if they correctly correlate multiple sensor inputs. Sensor networks aggravate the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance and can gather information in a low-risk, anonymous manner.

Traffic analysis: Traffic analysis always combines with the monitoring and eavesdropping. An increase in the number of transmitted packets between certain nodes could signal that a specific sensor has registered activity. Through the analysis on the traffic, some sensors with special roles or activities can be effectively identified.

Attacks against authenticity and integrity: Without proper authentication mechanisms, unauthorized people or devices could request services or data of the unprotected sensor nodes. In many cases these services or data may not be public. Malicious users could also try to join the network undetected by impersonating as some other trusted node. As a trusted node, it will now have access to private data or it can disrupt the normal network operations. As important as authenticity of origin (entity authentication) is the authenticity of data (message authentication or integrity). It should be guaranteed that sensor readings are transferred from sensor nodes to the gateways without any modification. Otherwise, wrong data will be processed resulting in incorrect decisions taken in operation centers and this might have disastrous effects such as directing military troops to the wrong side of the battlefield. Attacks on WSN routing protocols: For the sake of simplicity, almost none of the sensor network routing protocols do not consider security. As a result, WSN routing protocols are susceptible to many kinds of attacks. Most of these networklayer attacks against sensor networks are summarized in Table 1 (Abd-El-Barr et al., 2005).

Selective forwarding: In a selective forwarding attack, malicious nodes may decline to forward certain messages and simply drop them with the aim that they are not propagated any further. The simplest form of this attack is when a

Mallikarjun Talwar et al.
Security threads and quality of service challenges for wireless sensor networks: A Survey,
Indian journal of engineering, 2014, 10(21), 15-23,

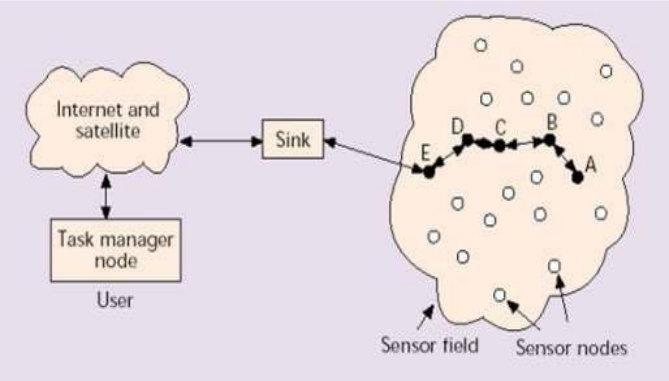

Figure 1
Operation of the sensor network

malicious node acts like a black hole and refuses to forward any packet. But, in that case, neighboring nodes may conclude that malicious node has failed and decide to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. A malicious node interested in suppressing or modifying packets originating from a selected few nodes can reliably forward the remaining traffic and hide suspicion of its wrongdoing.

Sinkhole attack: In a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes on, or near, the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks like selective forwarding. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For instance, an adversary could spoof or replay an advertisement for an extremely high quality route to a base station.

Sybil attack: In a Sybil attack, a single node presents multiple identities to other nodes in the network (Douceur, 2002). The Sybil attack can significantly decrease the effectiveness of fault-tolerant schemes such as distributed storage, dispersity and multipath routing, and topology maintenance. Replicas, storage partitions, or routes believed to be using disjoint nodes could in actuality be using a single malicious node presenting multiple identities. Sybil attacks also pose an important threat to geographic routing protocols which require nodes to exchange location information with their neighbors. It is reasonable to expect a node to accept only a single set of coordinates from each of its neighbors, but by using the Sybil attack, a malicious node can pretend to be in more than one place at simultaneously.

Wormhole attack: In the wormhole attack (Hu et al., 2003), a malicious node tunnels packets received in one part of the network over a low latency link and replays them in a different part. Wormhole attacks usually involve two distant malicious nodes collaborating to understate distance between them by relaying packets along an out-of-band channel. An adversary located close to a base station can totally disrupt routing by creating a well-placed wormhole. The adversary can fool nodes who are normally multiple hops from a base station that they are only one or two hops away via the wormhole. This creates a sinkhole. Since the malicious node on the other side of the wormhole can artificially provide a high quality route to the base station, all traffic in the surrounding area will be drawn through it if alternative routes are less attractive. This will most likely be the case when the endpoint of the wormhole is relatively far from a base station.

HELLO flood attack: In a HELLO flood attack an attacker broadcasting HELLO packets to announce itself with large enough transmission power could convince every node in the network that the adversary is its neighbor. For instance, a malicious node advertising a very high-quality route to the base station could cause a large number of nodes to attempt to use this route, but those nodes sufficiently far away from the adversary would be sending packets into a nullity. The network can enter into a state of confusion. Even if a node realizes the link to the adversary is false, it has not too many options because all its neighbors might be attempting to forward packets to the adversary as well. Protocols which depend on localized information exchange between neighbor nodes for topology maintenance or flow control are also subject to this attack. Acknowledgement spoofing: Many WSN routing algorithms rely on implicit or explicit link layer acknowledgements.

Physical attacks: Sensor networks usually operate in hostile outdoor environments. In such settings, the minimality of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks. Different from many other attacks mentioned above, physical attacks may destroy sensors permanently and the losses can be irreversible. For example, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker. Recent work has shown that today's standard sensor nodes, the MICA2 motes, can be compromised in about only one minute (Hartung, 2004).

6. SENSOR NETWORK APPLICATIONS REQUIRING BOTH QOS AND SECURITY

The first example of a WSN setting where both QoS guarantees and security is desired can be given as the previously mentioned real-time target tracking application in a battle environment (Younis et al., 2004). In such a scenario, lots of sensors are deployed in the battlefield in order to detect, identify, locate and then to track any object belonging to adversary like an enemy tank. Once this object is detected, for instance, by acoustic motion detection sensors, imaging sensors can be used to identify and locate it. After it is identified and located, video sensors can be turned on

Mallikarjun Talwar et al.
Security threads and quality of service challenges for wireless sensor networks: A Survey,
Indian journal of engineering, 2014, 10(21), 15-23,

to track the trajectory of this object while it ismoving. Since this object, let us assume that it is a tank, is moving in real-time, it is very important to send the video data about this tank with minimum possible delay so that its trajectory can be observed accurately in real-time. In addition, sending video data of this tank requires a certain amount of bandwidth for an acceptable image quality. These requirements regarding delay and bandwidth indicate that this application needs some kind of service differentiation to guarantee a certain degree of QoS, which, in turn, will ensure the proper operation of the deployed sensor network. Furthermore, in this scenario, protection of the security of the data is vital to the proper operation. For instance, an undesirable situation can occur when the adversary is able to modify the data in transfer to lead the owner of the WSN into confusion. For example, by modifying the sensed video data, the adversary may fool the control center of the WSN into thinking that the tank is moving in the opposite direction. This may result in directing the troops into the wrong direction whose consequences may be disastrous. Therefore, in this military target tracking WSN application, providing both QoS at network level and security is almost an obligation for proper operation of the network.

The second example is from a health monitoring application. Wireless Body AreaNetworks (WBAN) are composed of a large number of sensor nodes deployed over or inside the human body (Jovanov et al., 2005). Those sensors are usually implanted tiny medical devices monitoring and sensing signals from the human body to provide health data in real-time. For example, in a heart monitoring application sensors measuring blood pressure are used. This WBAN application monitors blood pressure of patients with heart attack risk to see if there are blood pressure abnormalities anywhere on the body. Medical data measured by those sensors, i.e., blood pressure as given in the example, is transmitted to the control center of a medical institution usually via a common RF link, i.e., cellular system. Physicians observe this data in real-time for any possible in-body disorder. If any problem is detected, further data can be requested by physicians to make a diagnosis and even some medical actions can be taken remotely through the actuators also deployed inside the body. In case of abnormal conditions in patient's health detected at the control center, i.e., a heart attack, more intense monitoring of certain vital signs might be required and more sensors may be required to be active in the current vicinity of the monitored object, i.e., heart. Therefore, an increased spatial resolution might be needed compared to normal cases where data sent by smaller number of active. The third example of a WSN setting where service quality and security requirements exist is an environmental surveillance application in which sensor networks are utilized. In authors consider a real time forest fire detection application to identify and precisely locate the fire site as well as define an efficient approach of intervention. A certain amount of sensors are used to measure the temperature throughout the forest to detect any signs of a fire (Trevis et al., 2004). Once an abnormally high temperature is measured over a certain area, number of sensors making measurements in proximity of this region is increased in order to provide more specific information about the fire such as the location, the direction and speed of its spreading, and this information is immediately relayed to the control center of the sensor network. Therefore, this application needs QoS guarantees at both network level (minimal latency in order to trigger the fire brigade closest to the fire with the least possible delay) and at application level (increased spatial resolution to provide detailed information about the fire).The security requirements about this WSN scheme are mostly related to the protection of authenticity and integrity. The sensor nodes which alarm the start of a fire should be authenticated to prevent any false alarms initiated by malicious nodes. Again, the transmitted data should not be able to be modified by anyone not to cause misleading of fire-suppressing teams to areas where there is no sign of a fire. Thus, it can be concluded that this environmental monitoring application is another sensor network setting where security and quality of service is needed at the same time. As can be seen from the three examples of possible WSN applications given in this subsection, there will be several instances where QoS and security should be provided simultaneously for a sensor network deployment. Thus, it is indeed a necessity to construct schemes which jointly provide security and QoS for wireless sensor networks

7. CHALLENGES IN PROVIDING BOTH QOS AND SECURITY FOR SENSOR NETWORKS

The challenges to provide QoS for sensor networks and the difficulties to make sensor networks secure were given previously. All of these challenges apply when one tries to mutually achieve QoS and security for wireless sensor networks. In addition to those, some extra challenges exist in simultaneously providing security and QoS for WSN applications due to the remarkable interactions between these two concepts. Particularly, degrading effect of security on some QoS parameters complicate the problem of mutual achievement of QoS and security. In this subsection, these additional difficulties related to the security-QoS correlation willbe covered. , when a network is unavailable meaning that authorized users cannot access the services when needed, the amount of QoS provided by this network can be said to be zero. Although the availability of a network can be harmed by interruption of communication links or failure of some nodes, DoS attacks are the most important threat to service availability. Jamming or energy deprivation attacks described in previous sections may diminish the performance of the network such that expected services cannot be delivered in a healthy way and users/applications receive unpredictable service quality. With a

Mallikarjun Talwar et al.
Security threads and quality of service challenges for wireless sensor networks: A Survey,
Indian journal of engineering, 2014, 10(21), 15-23,

secure system, however, which is resilient to DoS attacks, availability of the network is sustained even under attack, and therefore, QoS can still be guaranteed. As a consequence, security measures.

Negative Effects of Security on QoS: The standard approach to provide security to any system is to use of cryptographic primitives such as message integrity codes (MIC), digital signatures, one-way hash function, etc. The use of cryptography will mainly have two effects on the performance. The first one is due to the increased overhead in the length of the messages sent and the second one is due to the extra computational demands on the processor. The increased message size causes an increase in packet latency, decrease in throughput and an increased use of available bandwidth. And, the computational overhead results in more latency. These adverse effects are detailed below. The security methods such as MIC or digital signatures append additional bytes at the end of the data packets to be used in verification at receiver's side. These packet overheads are generally in the range of 8-32 bytes and therefore inconsequential for conventional data networks. However, for sensor networks, which have already little bandwidth available to use, packet size is usually small,i.e., 30 bytes in Berkeley's MICA motes. Therefore, a 8-byte security overhead is almost 25% of the total packet size and has several effects on the QoS of the sensor network. Firstly, longer packets occupy more bandwidth leaving less available bandwidth for QoS constrained traffic. Moreover, large packets circulating in the network cause an increase in the total traffic load present in the sensor network. This increased amount of packet traffic may cause congestions onintermediate sensor nodes which forward packets. This congestion not only decreases the average throughput of the network but also causes increased overall delays due to the higher queuing times of congested nodes. The increase inlatency is contributed also by longer transmission times of longer data packets. Another element causing degradation of QoS parameters is the computational burden put on the sensor node's processors by cryptographic methods like encryption. Although it varies according to the used cipher algorithm, encryption process usually involves lots of arithmetic and logic operations. These operations take thousands of CPU cycles to be completed by the processor. For Giga-Hertzspeed processors used in conventional computers like PCs and laptops, these calculations are not too cumbersome (Guimaraes et al. 2005).

Positive Effects of QoS on Security: Though it is not as intuitive as for the case of security's effect on QoS, employing QoS mechanisms have some contributing impacts on network security. One of these positive effects cited in Bhattacharya et al., (2000) is the prevention of covert timing channels. A covert channel is anunintended communication channel that may be used to transfer data in a manner that violates the security policy. A potential covert channel is a timing channel ifits use involves a process that signals information to another process by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process. Ifa QoS policy provides certain bounds for delay or latency; covert timing channels cannot be utilized by malicious a node, which in turn contributes to the security.Another positive effect of QoS on security mentioned in Sakarindr et al., (2005) is the following. A finely tuned QoS policy that provides certain amounts of bandwidth for some defined types of traffic can detect unusual network traffic caused by some malicious nodes that are launching an attack. If QoS and security systems are in cooperation and can share information, QoS system can alert the security system about the existence of this out-of-profile traffic that is not in accordance with defined QoS policies, and thus help the security system to detect and prevent this attack.

8. CONCLUSION

WSAN is an area still in its infancy, despite some recent progress. It is anticipated that WSANs will evolve rapidly and become pervasive in the near future, much in the same way as the Internet came to the desktop before. Lessons should be taken from Internet that WSANs have to be designed with QoS support in mind. This paper has discussed the requirements and challenges for supporting QoS in WSANs. Some interesting open research topics have been identified, though the spectrum of research in this field can be much broader. The challenges are formidable and extensive research from multiple disciplines is needed before QoS-enabled WSANs become reality.

REFERENCES

1. Abd-El-Barr, M. I., Al-Otaibi, M. M. & Youssef, M. A. (2005). Wireless Sensor Networks - Part II: Routing Protocols and Security Issues. Proceedings of the 18th IEEE Annual Canadian Conference on Electrical and ComputerEngineering (pp. 69-72)
2. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. & Cayırcı, E. (2002). Wireless
3. Chen, D. & Varshney, P. K. (2004). QoS Support in Wireless Sensor Networks: A Survey. Proceedings of International Conference on Wireless Networks 2004 (pp. 227-233)
4. Douceur, J.R. (2002). The Sybil attack. Proceedings of the 1st International Workshop on Peer-to-Peer Systems (pp.251-260).
5. Guimaraes, G., Souto, E., Kelner, J. & Sadok, D. (2005). Evaluation of Security Mechanisms in Wireless Sensor Networks. Proceedings of International Conference on Sensor Networks (pp. 428-433)
6. Hartung, C., Balasalle, J. & Han, R. (2004). Node compromise in sensornetworks: The need for secure systems (Technical Report CU-CS-988-04).Colorado, US: University of Colorado at Boulder, Department ofComputer Science.
7. Hu, Y.-C., Perrig, A. & Johnson, D.B. (2003). Packet leashes: a defense against wormhole attacks in wireless networks. Proceedings of the IEEE Infocom,2003 (pp. 1976-1986)

Mallikarjun Talwar et al.
Security threads and quality of service challenges for wireless sensor networks: A Survey,
Indian journal of engineering, 2014, 10(21), 15-23,

8. Jovanov, E., Milenkovic, A., Otto, C. & Groen, P.C. (2005). A wireless body areanetwork of intelligent motion sensors for computer assisted physical rehabilitation. Journal of NeuroEngineering and Rehabilitation, 2(6)
9. Kuorilehto, M., Hannikainen, M. & Hamalainen, T.D. (2005). A Survey of Application Distribution in Wireless SensorNetworks. EURASIP Journal on Wireless Communications and Networking, 2005(5), 774-788
10. Shah, R. & Rabaey, J. (2002). Energy Aware Routing for Low Energy Ad HocSensor Networks. Proceedings of IEEE Wireless Communications and Networking Conference 2002 (pp. 350-355).
11. Trevis, L. & El-Sheimy, N. (2004). The Development of a Real-time Forest Fire Monitoring and Management System. Proceedings of the 20th Congress of International Society for Photogrammetry and Remote Sensing (pp. 65-71).
12. Walters J.P., Liang, Z., Shi, W. & Chaudhary, V. (2006). Wireless sensor network security: a survey. In Y. Xiao (Ed.), Security in distributed, grid, and pervasive computing (pp. 367-411). United States, FL: Auerbach Publications.
13. Wood, A. D. & Stankovic, J. A. (2002). Denial of service in sensor networks.Computer, 35(10), 54–62.
14. Younis, M., Akkaya, K., Eltoweissy, M. & Wadaa, A. (2004). On Handling QoSTraffic in Wireless Sensor Networks. Proceedings of the Proceedings ofthe 37th Annual Hawaii International Conference on System Sciences (pp.10-16).

Mallikarjun Talwar et al.
Security threads and quality of service challenges for wireless sensor networks: A Survey,
Indian journal of engineering, 2014, 10(21), 15-23,