Computer and Information Science; Vol. 13, No. 2; 2020
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Security of Broadcast Authentication for Cloud-Enabled Wireless Medical Sensor Devices in 5G Networks

Abdullah Al Hayajneh[1], Md Zakirul Alam Bhuiyan[2] & Ian McAndrew[1]

[1] Capitol Technology University, MD, USA

[2] Fordham University, NY, USA

Correspondence: Abdullah Al Hayajneh, Department of Doctoral Programs, Capitol Technology University, Laurel, MD 20708, USA.

Received: March 5, 2020 Accepted: March 18, 2020 Online Published: March 26, 2020

doi:10.5539/cis.v13n2p13 URL: https://doi.org/10.5539/cis.v13n2p13

Abstract

Wireless Body Area Network (WBAN) has become one of the fastest growing technologies nowadays. There are some characteristic limitations in WBAN, especially when it comes to health-related applications that are used to monitor human bodies. To overcome and mitigate theses limitations in WBAN, cloud computing technology can be combined with the WBAN as a solution. We can classify the WBAN sensors in the cloud-based WBAN into i) nodes that monitor the human body and ii) WBAN actuators that take action upon the order commands from the medical staff. The biggest concern is the security of the medical commands to the WBAN actuators because if they are altered or tampered with, there can be serious consequences. Therefore, authentication plays an important role in securing cloud-based WBANs. In this article, we explore the security and privacy issues of Wireless Body Area Network combined with Mobile Cloud Computing (wMCC) with 5G mobile networks and investigate public-key based security solutions. At first, the paper presents a detailed description of wMCC architecture, discussing its main advantages and limitations. The main features of 5G mobile network are then presented, focusing on the advancement it may provide if integrated with wMCC systems. We further investigate the security issues of wMCC with 5G mobile networks while emphasizing the challenges that face this system in healthcare applications. The authentication techniques in wMCC are then classified and discussed with the feasibility of deploying practical solutions. Finally, we outline the main challenges and metrics of an ideal authentication protocols to be used in wMCC with 5G. The metrics are helpful for researchers in this field to evaluate, analyze, and compare the authentication protocols to decide the suitable application for each protocol.

Keywords: WBAN, WSN, broadcast authentication, security, privacy

1. Introduction

Recent advances in wireless communication allow mobile networks to reach higher levels in bandwidth and Quality of Service (QoS) performance. This accelerating development makes them compete with traditional networks, given the ease of installing and setting up wireless networks. This technology evolution is also accompanied by new bandwidth-hungry and QoS-demanding applications. Pervasive healthcare is a particular application that may extensively benefit from this evolution.

A relatively new cloud-computing technology can help in securing, storing, and reporting data (Almashaqbeh et al., 2014). Due to its abundant resources, cloud computing provides an efficient solution to address big data storage and analysis. Accordingly, to overcome the battery, processing, and storage limitations of mobile devices, cloud computing is integrated with the mobile environment to form what is known as Mobile Cloud Computing (MCC) (Rahimi, 2014; Karaca, 2019). The resultant product of this merge significantly promoted the performance of the mobile networks and paved the way for a new era of applications, especially in medical systems.

Wireless body area network (WBAN) is a technology that provides an effective and cost-efficient solution for remote health monitoring. Typically, a WBAN consists of several sensor nodes that are attached in, on, or around a human body to report a variety of important physiological measurements (Chen et al., 2011). Storing and processing data in the WBAN in local networks creates complications in WBAN architecture. MCC offers several options and promotions for medical sensor devices that can overcome these limitations (Fortino et al., 2014).

The resultant system from merging Mobile Cloud Computing (MCC) with WBANs is referred to as cloud-enabled WBANs. It is a fact that mobile health monitoring with cloud-based computing is much faster and less power consumption than the mobile health monitoring that operates independently (Ahnn & Potkonjak, 2013). Although mobile healthcare with MCC in medical WBAN minimizes limitations of traditional medical devices in terms of small physical storage, security, and privacy (Dinh et al., 2013), some challenging issues remain with this merge. In particular, providing a high level of QoS and performance that meets the requirements of intensive healthcare applications is still not fully achieved. The security and privacy of healthcare applications is yet another critical issue to be solved.

The 5G mobile network is a growing technology that is in the process of becoming standardized. This generation of mobile internet connectivity promotes fast, reliable, and more efficient service compared to the previous generation of networks such as 3G and 4G. This 5G technology will allow for a huge amount of data to be carried in the network for a smarter connected world (McCann, 2020). Researchers discussed the challenges of converting to 5G technology, including the high cost and the non-confidence of the multinational companies on how to cover this high cost in the near future. To solve that, the researcher proposed a centralized data center structure and economic model solution to improve and lower the high cost of 5G technology (Patwary et al., 2020). The prospective vision is to connect the global world everywhere and with billions of devices of all types. Operating MCC under 5G mobile network infrastructure will certainly promote the efficiency of Wireless Body Area Network combined with Mobile Cloud Computing (wMCC) in terms of QoS and performance and will make it capable of meeting the needs of the new extensive healthcare applications.

In this article, we explore the security and privacy issues of wMCC with 5G mobile networks and investigate public-key based security solutions. At first, the paper presents a detailed description of wMCC architecture, discussing its main advantages and limitations. The main features of the 5G mobile network are then presented, focusing on the advancement it may provide if integrated with wMCC systems. We further investigate the security issues of wMCC with 5G mobile networks while emphasizing the challenges that this system faces with healthcare applications. The authentication techniques in wMCC are then classified and discussed where the feasibility of deploying the Rabin algorithm is experimentally studied. Finally, we outline the main challenges and metrics of an ideal authentication protocol to be used in wMCC with 5G. The metrics and analysis for broadcast authentication are helpful for researchers in this field s to decide the suitable application for each protocol.

2. wMCC Model

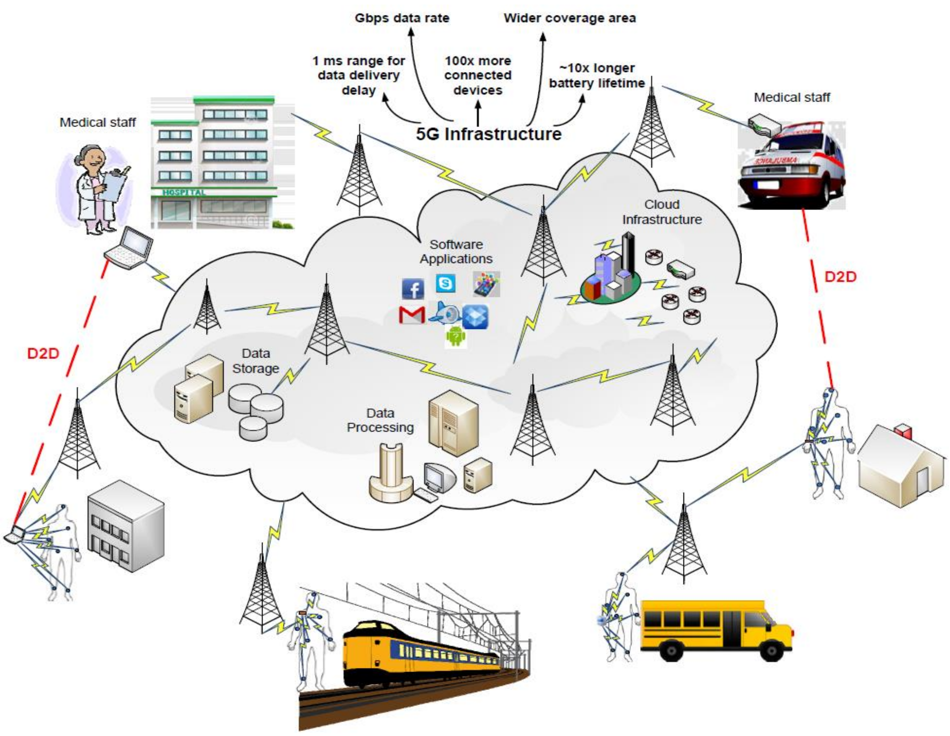

Figure 1. Cloud-based WBAN Architecture with 5G

The 5G mobile networks are in the process of becoming standardized and characterized by being all IP with high throughput and IPv6 as the basic protocol. Since billions of devices will be on the 5G network, some of the main technical requirements of 5G will be as follows (Khan et al., 2019):

- Higher system capacity.
- Higher data rates.
- Lower latency.
- Efficient processing to support low power devices.
- Support devices with limited communication capabilities.
- Higher traffic density and coverage.
- Higher accuracy to support outdoor and indoor devices.

In addition, as shown in Figure 1, 5G mobile networks are expected to provide new services such as a direct device to device (D2D) service where communication equipment can directly exchange data traffic with another device without going through base stations or the core network. Some assistance can be used to setup a direct connection. This service facilitates new applications, including social networking, peer-to-peer content sharing, and most importantly, public safety communications in the absence of network coverage. Researchers discussed the 5G technology solution to improve the handling of the big data coming from smart home network sensors and make it adaptable to the current available infrastructures in the market (Lynggaard & Skouby, 2015). (Zhang & Lin, 2017) discussed the device to device communication technology in 5G networks, and it’s security problems and threats. They proposed security solutions and frameworks to improve the security in the application and physical network layers for the 5G networks. Other researchers proposed a new 5G authentication protocol to conquer the current version of the Authentication and Key Agreement Protocol for 5G (Braeken et al., 2019).

In summary, 5G mobile networks aim to support higher bandwidth and speed with minimal delay. Accordingly, operating wMCC with 5G will enhance the performance of health applications that use WBANs. That is, the high system capacity and data rate allows WBAN sensors to report the measurements of the human body more frequently and with large data such as medical images or video streaming. In addition, the lower latency allows for interactive health applications that require immediate intervention from the medical staff based on the reported data. Moreover, the high speed and large bandwidth provided by 5G mobile networks will allow the medical staff to locate the cloud side to require more detailed data from the WBAN sensors to better diagnose the patients. Further, it allows the medical staff to send instant commands to the WBAN actuators in order to perform necessary medical interventions. The later is possible with the D2D 5G service where medical staff can directly contact the WBAN actuator device or have the WBAN directly contact an ambulance in case of an emergency.

3. Security Issues of wMCC in 5G

In this paper, we consider the implementation and evaluation of a security mechanism that is suitable for cloud-based WBAN. We consider the performance of the relay master nodes that do not verify or sign messages commands, and smart master nodes that perform these tasks.

Typically, MCC is expected to inherit all security issues existing in conventional cloud computing. The following are the main security issues in MCC (Fernando, 2013; Zissis, 2012; Jones, 2018):

Trust is an essential component in building any secure system. It implies that each of the two communicating parties expects the other party to behave as required. In cloud-computing, data is processed and stored outside the organization's network, which jeopardizes trust in that communication. Thus, many researchers proposed relying on a Trusted Third Party (TTP) and using cryptography to address the trust issue.

Confidentiality and privacy mean that only authorized users are allowed to access protected data. Due to the large number of involved parties in cloud-computing, there is a higher possibility for the data to be compromised in the cloud. Data confidentiality is also related to user authentication as unauthorized access may cause invasion of data privacy.

Integrity and authentication are other important factors. While integrity implies that exchanged data is protected from any malicious modification, deletion, or fabrication, authentication means that the claimed message sender is the actual party who sent the message (i.e., no impersonation). Again, in cloud-computing, assuring the integrity of the data while being saved and processed at the remote servers and preventing anyone from impersonating a sender are critical issues.

Availability is to guarantee that all the system resources are available and accessible to authorized users whenever needed. Cloud-computing data may be distributed and stored at various locations that are maintained by different administrative authorities, making availability a challenging issue.

Trusted Third Party (TTP) is a centralized trusted authority that can help to establish an adequate trust level and maintain the confidentiality, integrity, and authenticity of the data and communication. Relying on a trusted third party is a suitable option for the cloud computing infrastructure and requires using digital certificates with public-key cryptography.

Other vulnerabilities in MCC are possible attacks related to the characteristics of mobile devices and the usage of wireless communication channels. Examples include battery exhaustion attacks, mobile botnets, targeted attacks, and the injection of fake and fabricated messages. Further, attacks that violate the MAC layer standards causing DoS are also easy to launch in this case. Hu et al. (2019) discussed the several types of DoS attacks that can occur on the 5G network devices.

As elaborated earlier, mobile healthcare applications are generally demanding in terms of battery, storage, and computation. Using MCC is an efficient solution for these limitations. However, security remains a prominent issue between the two sides (i.e., the cloud computing and the mobile device) with patients data and location confidentiality being the most critical of all issues, especially when processed by an external tool at a remote server. Fortino el at., (2014) have advised three levels of security for cloud-assisted WBAN: at the sensor data collection, transmission, and management and access levels. Transmission of WBAN data must be secured from any potential intruders.

Connecting medical devices and wireless medical sensors to the internet and cloud services enhanced the efficiency and quality of the healthcare environment. However, this connection increased medical device hacking as it allows hackers to attack from all over the world through the internet. In 2017, the U.S. Food and Drug Administration (FDA) recalled around half a million peacemaker medical devices, which help patients to control their heartbeat because of security vulnerabilities that were found on these devices (McKinley, 2020).

Moreover, the patient's data integrity should be maintained to guarantee that it is not mistakenly mixed with other patients. Shin & Kwon, 2018 proposed and designed network architecture and a dual-factor authentication for 5G-integrated with WSNs for the Internet of Things. They reviewed another research security schema made by Tai et al. (2017) and discussed the weaknesses and vulnerabilities of it. Then proposed a dual-factor authentication for 5G integrated WSNs. The research evaluation shows an improvement in the security aspects without the need to make a significant change in any security schema on IoT devices.

4. Classification of Authentication in wMCC

In this paper, authentication refers to both source and data authentication. Source authentication guarantees to the receiver that the message originated from the actual sender. Data authentication grants that the contents of the message were unchanged, also called message integrity. Authentication mechanisms are very important for WBAN/WSN applications to ensure that messages originated from legitimate nodes and their contents were not altered during the transition. For example, in a fire alarm sensing system, it is not important to ensure the confidentiality of a message but very important to ensure that no messages are injected to cause a false alarm. Thus, it has been argued that authentication is the most important security requirement in WBAN/WSN. Broadcast authentication in WBAN/WSN could be defined as a mechanism to send authenticated messages or commands to many sensors, or probably to all the sensors in the network. Moreover, the base-station needs to send authenticated commands or query messages, using a cryptographic key, to all the sensor nodes in the network. The base-station will directly send the message to the nodes that are within its transmission range and those nodes will forward the messages to their neighbors until all the nodes in the network receive the message. Each sensor node, upon receiving the message, has to use the authentication information to verify the authenticity of its origin and contents, using the same or different cryptographic key.

Throughout this paper, we will refer to the base-station and the sensor nodes as the sender and the receivers, respectively. Broadcast authentication is essential in WBAN/WSN because it will ensure that only the base-station will generate commands or query messages and will guarantee that their contents are intact. Without broadcast authentication, malicious code can impersonate the base-station or an attacker can change the broadcasted messages to make the sensor nodes perform actions that they are not supposed to do. Furthermore, many important applications in WBAN/WSN rely on secure broadcasting, such as network management, routing tree construction, software updates, time synchronization, and network query.

As discussed earlier, authentication of commands in wMCC sent to WBAN sensors or actuators is the most critical security issue. One of the main security measures taken by WBAN nodes involves authentication of a signed message; therefore, the best option to have a quick and effective signature process is through the use of a public-key scheme.

Authentication protocols in WSN/WBAN (Luk at al., 2006) can be classified by the cryptographic primitives they use, as shown in figure 2. The first type is protocols that use symmetric cryptography, also referred to as secret key cryptography, in which the sender and the receiver(s) share a secret key.

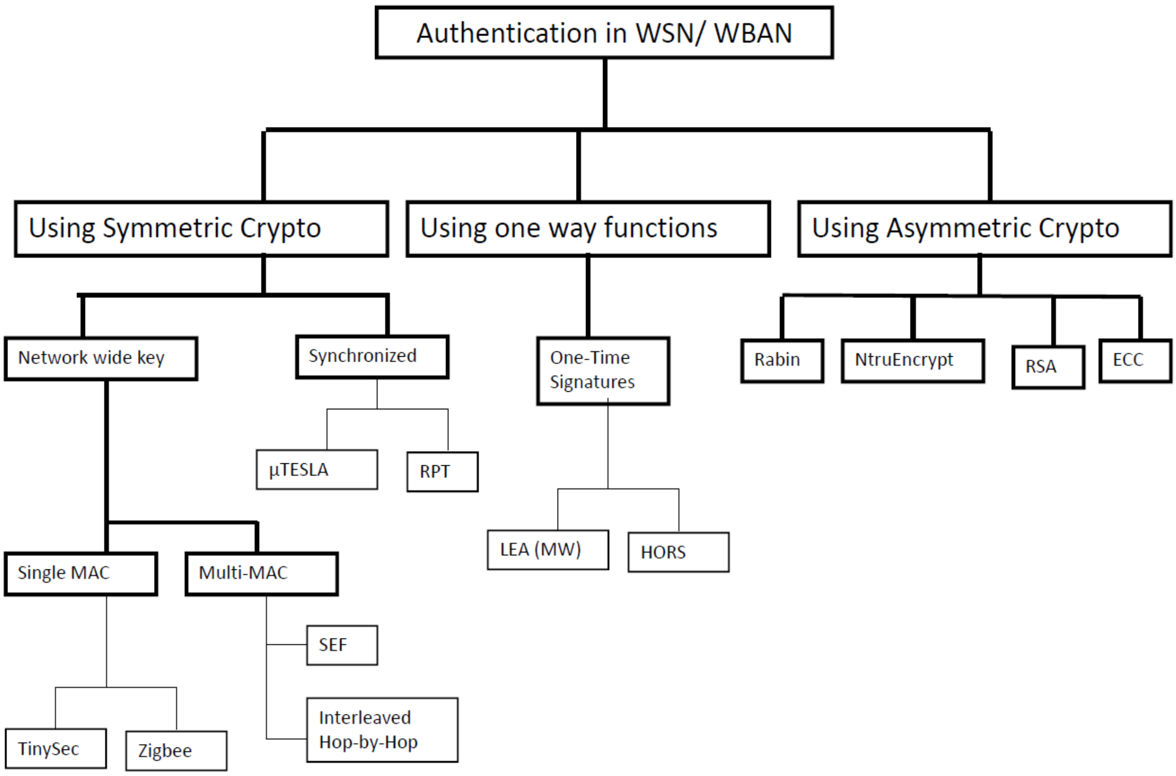

Figure 2. Classification of Broadcast Authentication Protocols in WSNs

Symmetric cryptography is preferable in low-resource devices as WSN and WBAN because they require moderate computation, which makes them run faster and consume less power. The most common standardized protocols are TinySec and Zigbee. Both were designed mainly to provide secure peer-to-peer communication. For broadcast authentication, they use a network-wide key to compute message authentication code. However, broadcast authentication inquires asymmetry to prevent any of the receivers from impersonating the sender. Some symmetric cryptographic protocols, referred to as synchronized protocols, use time delays to achieve this goal, but introduced new limitations. They require the node to be strict time synchronized and cause delays in the authentication process, which is a critical issue for healthcare applications.

The second type of protocol uses one-way functions to implement one-time signatures. They are fast and efficient but produce high communication overhead. The last type of protocol uses public key cryptography and is considered the default for achieving asymmetry in authentication and broadcasting authentication for conventional networks. A decade ago and due to the expense in storage and computation, public-key cryptography was not a practical approach in WSNs. However, as will be shown in this paper, recent studies together with the hardware enhancement in WBAN sensors, public key cryptography may become the future solution for authentication in WBAN.

As for protocols that use public key cryptography and one-time signature, the public key of the sender can be known only to one node or to all the nodes in the WSN. For a protocol that uses symmetric shared key the problem becomes a key management issue. If the key is a pair-wise key, then it can be used to authenticate messages between two sensors. On the other hand, if the key is a network-wide key known to all the sensors, then it can be used to broadcast authentication. Thus, it is more efficient to use the pair-wise key for authentication since using other protocols such as synchronized protocol requires additional services such as time synchronization for all the sensors in the WSNs.

4.1 Performance Metrics of Broadcast Authentication

In this section, we will outline the main challenges and metrics of an ideal authentication protocol to be used in wMCC with 5G. The metrics will be helpful for researchers in this field to evaluate, analyze, compare the protocols and decide the suitable application for each protocol. The challenges and metrics for authentication include the following (Alhayajneh, 2018; Luk, 2006):

(1) **Short authentication delay**. Most of the healthcare applications require real-time response; for example, WBAN deployed in a human body to measure the blood sugar; it may be necessary to increase the insulin dose in the blood immediately. This implies that authentication should be immediate with minimal if any, additional messages needed to authenticate a message.

(2) **Robust to packet loss**. The wireless links between the WBAN nodes and the master node are prone to high bit-error-rate and signal fading; therefore, the protocol must take into consideration packet loss and be capable to rapidly recover any potential packet loss.

(3) **Resilience against node compromise**. In most WBAN applications, the sensors are deployed in an unsecured environment where they are vulnerable to physical attacks. It is possible for an attacker to capture a node or more and to extract their cryptographic keys. It is essential for the broadcast authentication protocol to be resilient and cope scenarios when an attacker deploys replicated compromised nodes to perform a malicious action.

(4) **Low communication overhead**. Transmission is the most energy consuming action that a WBAN sensor performs where energy is very constrained. Moreover, WBAN node's energy will impact the lifetime of the network. Consequently, to attain a long lifetime for the WBAN, the protocol must not involve large communication overhead.

(5) **Low computation cost**. Computation is much less energy expensive than communication in WBAN. However, it is still preferable for the protocol to be computationally inexpensive as this may also cause time delay.

(6) **Low storage requirement**. The storage space in WBAN sensors is very limited and the protocol must be designed not to exceed or fill out the memory capacity. Memory processing and management may also result in time delay and energy consumption.

(7) **Independent authentication**. The failure to authenticate one packet should not affect the authentication of other packets. The packets must be individually authenticated and independent of other packets.

(8) **Immunity to DoS attacks**. DoS is a common attack in wireless networks; thus, the protocol must be survivable to adapt its operation and deliver authenticated messages under DoS attacks.

(9) **Scalability** (in terms of both, number of receivers and senders). WBAN consists of a large number of nodes and the protocol must be scalable to provide services for large number of receivers. Moreover, with upcoming 5G mobile networks, the number of nodes are expected to increase significantly which makes this issue concern.

4.2 Public-key Cryptography in wMCC

Public-key cryptography, also known as asymmetric cryptography, is a candidate solution for the security issues in wMCC. In this case, each node has two keys, i) a private key, only known to the key owner, ii) a public key, known to every node in the network.

A major security concern in any cloud-based WBAN model is to make sure the received commands to the WBAN actuators are issued by the certified medical staff without any interruption. We believe that using public key cryptography can be effective in securing a large number of WBAN nodes that are widely distributed and easily inserted or removed. Figure 3 shows the public key security model. The WBAN node needs the public key of the medical staff to process the commands. However, while using the public key system works well in terms of authentication and security, it could potentially overload and be heavy on the WBAN nodes, which might cause delays and energy consumption.

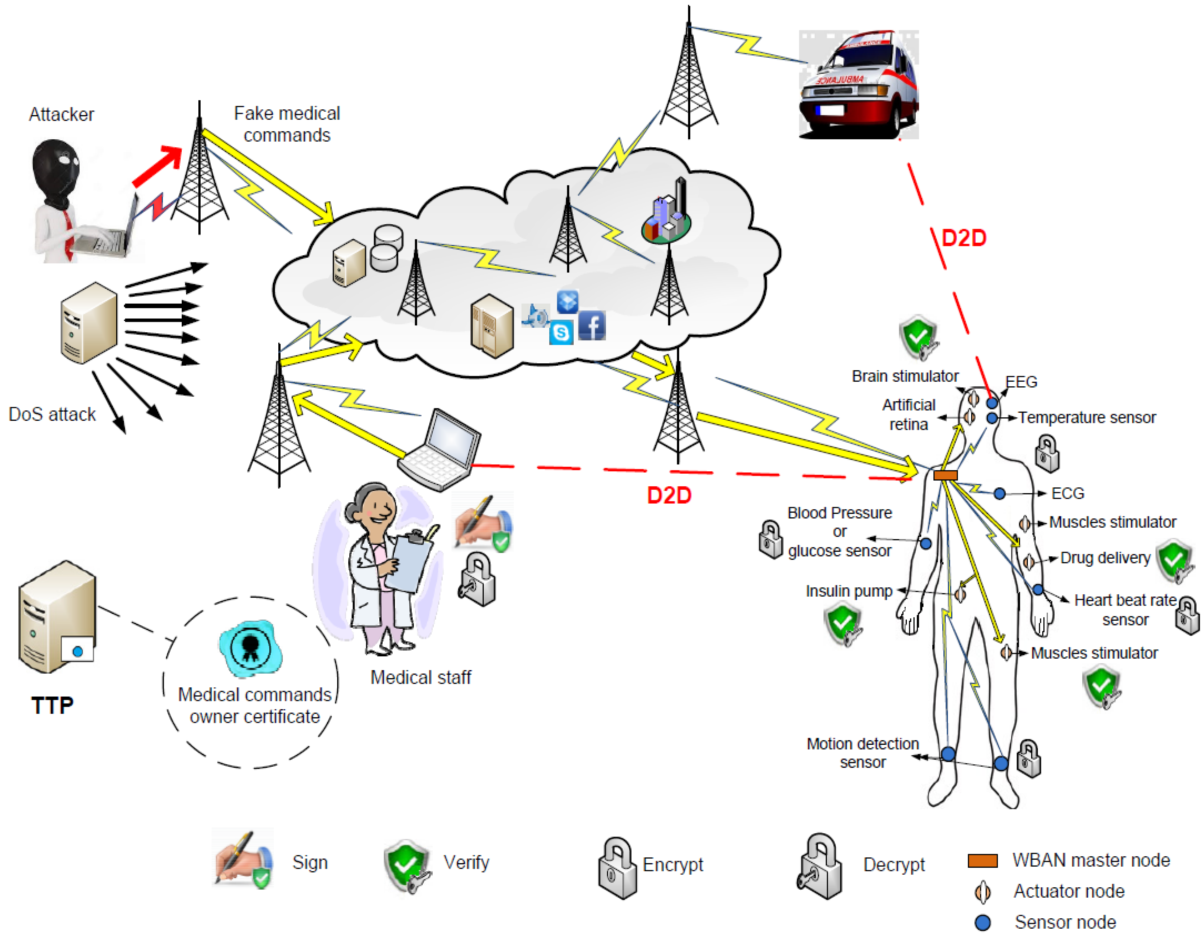

Figure 3. wMCC in 5G Security Model

5G mobile networks have the D2D service, which allows the medical staff devices to directly contact WBAN sensors and actuators. Thus, we need a mechanism to verify these commands and ensure their authenticity. In this case, it may be preferable not to trust the mobile device to issue the command as it might be corrupted with viruses or some malicious software. The command can either be sent directly to the WBAN node or relied on some master node to be verified at the WBAN device.

Relaying on a TTP is a suitable solution for cloud-computing infrastructure. The TTP, in this case, will issue digital certificates for the medical staff that they will send to the WBAN. The WBAN will verify the certificates with the public key of the TTP. Then the medical staff can send its commands signed by their own private key. In what follows, we discuss and classify the authentication protocols in wMCC.

4.3 Public-Key Cryptography and Network Lifetime

Using public key cryptography, specifically Elliptic-Curve Cryptography (ECC), in broadcast authentication is more secure and reliable compared to secret key cryptography. The only limitation is that they are computationally expensive, which implies that they consume more energy. That will drain the finite energy of the sensor nodes. The WSN lifetime depends on the lifetime of the sensor's batteries in the WSN (Nayak & Devulapalli, 2015). It can be defined when the first sensor battery is drained of energy. Thus, in this section, we will show how public key cryptography will influence the WSN lifetime.

Piotrowski et al. (2006) investigated the cost of public key cryptography in WSN and its influence on the node's lifetime. They revealed interesting results in which they agreed with previous researchers that RSA (Rivest–Shamir–Adleman) cryptography is not really reasonable in WSN. This is due to the enormous time, computation, communication overhead, and thus energy it requires. Table 1 (Piotrowski et al., 2006) shows the power consumption and time consumed for signature generation and verification on MICA2DOT sensors.

Table 1. Signature timing of public broadcast authentication

Cryptosystem	Signature –Power		Signature - Time	
	Generation	Verification	Generation	Verification
RSA-1024	304.0 mWs	11.90 mWs	23.03 s	0.86 s
ECC-160	22.8 mWs	45.1 mWs	1.65 s	3.27 s
RSA-2048	2302.7 mWs	53.70 mWs	166.86 s	3.89 s
ECC-224	61.54 mWs	121.98 mWs	4.46 s	8.84 s

Using MICA2DOT with 4400 Ws and TelosB with 6750 Ws of energy available by the double AA battery pack, Table 2 shows the estimated amount of signature generation and verification operations that could be accomplished before the power drops below the minimum level. The results are promising, for example, in the TelosB with ECC-160 if a signature is to generate every minute, then the sensor can last for 2 years. This lifetime is long enough for many applications.

Table 2. Complexity of public authentication

Cryptosystem	MICA2DOT		TelosB	
	Generation	Verification	Generation	Verification
RSA-1024	12105	310078	97867	2500000
ECC-160	161586	81542	1078275	543916
RSA-2048	1598	68547	12904	553279
ECC-224	59791	30166	398701	201192

5. Analysis and Applications for Broadcast Authentication Protocols

So far in this paper, we presented a detailed description of the broadcast authentication protocols in WSNs. In this section, we will compare and provide performance analysis for these protocols clarifying the applications in which each one can be best applied. Table 3 shows how each protocol category satisfies, does not satisfy, or partially satisfies each metric.

Table 3. Broadcast Authentication Protocol Metrics

	Metric 1	Metric 2	Metric 3	Metric 4	Metric 5	Metric 6	Metric 7	Metric 8	Metric 9
Net. wide key	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Synchronized	No	Partially	Yes	Yes	Yes	Partially	No	No	Partially
One-time sig.	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Partially
Public key	Yes	Yes	Yes	Partially	Partially	Yes	Yes	No	Partially

Broadcast protocols that use a network-wide key rely on symmetric cryptography, which makes them fast and of low computation cost. The sensors have to be inexpensive; therefore, it is impractical to equip them with tamper-proof hardware. In a hostile environment, an attacker can capture one sensor or more and exploit the secret key. Due to the absence of asymmetry, compromised nodes can forge messages or commands and broadcast them as if the base station generated them. In this scenario, an attacker can cause large damage to the WSNs. Standardized protocols as TinySec and Zigbee do not satisfy metric number third. Despite the vulnerability of these protocols to compromised node attacks, they are considered scalable in terms of both the number of senders and receivers. Broadcast protocols that use a network-wide key can be used for broadcast authentication only in physically secured areas. For example, an attended army base; where any attempt to capture or compromise a node is not possible.

In protocols with Multi-MAC, the compromise node problem will be critical if the sender calculated the MAC for each message using the same key that is shared with all the receivers. To overcome this problem, the sender can use a different key for each node to compute a different MAC per receiver and add them to each message. Using multi-MAC will degrade the problem of metric number three. It will challenge the attacker to capture and compromise a larger number of sensors and increase the chances of detecting the attack. On the other hand, this will raise another problem that dissatisfies metrics numbers four and five, resulting in consuming more power and decreasing the network lifetime. Consequently, the use of multi-MAC is considered impractical for WSNs.

Synchronized protocols also use symmetric cryptography but achieve asymmetry using time delays. They necessitate loose time synchronization between the sensors in the WSN. Researches in WSNs (Elson et al., 2002) accomplished accurate time synchronization in the range of µs, which is more accurate than the time synchronization required by µTESLA. In this case, if an attacker compromises a node, they cannot impersonate the base-station to inject forge messages or commands. This will ensure that metric number three is satisfied. The µTESLA family protocols will not fully satisfy metrics numbers 1, 6, 7, 8, and 9. To authenticate packets, the receiver must wait for the key disclosure period which is at least two-time intervals. Also, the receiver has to buffer all the received packets while waiting for the appropriate key. However, metric number two is satisfied because even if a packet with a needed key is lost, the receiver can compute the key from keys attached to packets sent at the next time intervals. Synchronized protocols are best applicable in applications where immediate response is not needed and messages are sent continuously in fixed periods. For example, it could be used in applications as structural health monitoring and habitat monitoring. In the former one, the base-station will periodically request measured data from the sensors. The data will be sent to a research center for analysis to decide whenever the structure needs any maintenance. Moreover, µTESLA was used to create functionalities in route discovery and maintenance procedures for WSN authentication in (Djellouli et al., 2020) and in (Wang et al., 2019) STEADY- µTESLA protocol has been proposed to secure for data quality and credibility in WSNs in cluster-based. Da Conceicao et al. (2017) used µTESLA protocol to secure and authenticate information communication exchange in vehicular networks.

One-time signatures are digital signatures that are normally used to sign one message. They were first invented by (Rabin, 1978) and (Lamport, 1979), respectively. One-time signatures are the fastest to perform signature verification. They require high communication overhead; this means consuming more energy, which is the most critical constrain in WSNs. Thus, for applications where nodes can be powered and the energy consumption is not an issue, a one-time signature would be a good choice. For example, if sensors are used for traffic lights monitoring, then the one-time signature can be fast and provides a good level of security. Benzaid et al. (2016) discussed several proposed schemes on the one-time signature mechanism, which shows that it requires large storage, and that also considered as a critical constrain in WSNs.

Finally, protocols with public key cryptography can provide a good and robust broadcast authentication in WSNs. For Rabin, NtruEncrypt and RSA protocols, the main concerns are the key sizes and high computational cost. They require key sizes of at least 1024-bit to provide 80-bit equivalent security, which is difficult to handle with the 8-bit processors. It will also result in large signatures causing communication overhead. Only, ECC uses small keys of 160-bit and acceptable computational cost for 8-bit processors. Sensors with 16-bit processors can easily manage ECC protocols, and they are not considered computationally expensive. These protocols provide the best match with the metrics of the ideal protocol for broadcast authentication in WSNs. Protocols with public key cryptography are considered scalable in terms of the number of receivers since new nodes only need to be initiated with the public key of the base-station. However, it is difficult to have more than one sender because all the nodes need to know the public key of the new sender. Researchers in (Du et al., 2005) proposed an efficient way to authenticate public keys in WSNs. Usually, this operation requires an expensive verification for a digital certificate. They proposed the use of a one-way hash function to perform public key authentication. However, they required that one-way hash values of the public keys to be securely exchanged prior to the deployment.

Protocols that use public key cryptography or require time synchronization are more vulnerable to DoS than other protocols. DoS attacks against broadcast authentication will be further discussed in the next section.

6. Attacks against Broadcast Authentication

Attacks in WSNs are not limited to broadcast authentication. For example, attacks against routing or MAC layer protocols may also disrupt broadcast authentication protocols. In this section, we will describe some attacks that mainly target broadcast authentication protocols and present prevention techniques that were suggested by researchers.

DoS attacks are common attacks in WSNs that target the protocols at all the stack layers. Aborujilah et al. (2019) studied and analyzed DoS attacks on WSNs and their defenses. Ning et al. (2008) studied the vulnerability of broadcast authentication protocols in WSNs to DoS attacks. They classified the broadcast protocols into two general approaches: digital signatures and μTESLA based techniques. In the case of signature-based broadcast authentication, an attacker can easily broadcast a large number of forged messages with a digital signature. Accordingly, the energy of the sensors will be consumed as they try to verify the signatures. In the case of μTESLA-based broadcast authentication, an attacker can exhaust the energy of the sensor nodes by forcing them to forward a large number of bogus packets. Moreover, Ning et al. also developed an approach to mitigate the DoS attacks against both μTESLA-based and signature-based broadcast authentication. In this case, the base station will compute an efficiently verifiable weak authenticator and add it to the broadcasted authenticated message. The receivers upon receiving the packets will check the weak authenticator, and only if it is verified, will they perform the expensive signature verification (in case of signature-based broadcast authentication) or forward the packet (in case of μTESLA-based broadcast authentication). The main drawbacks of this scheme are that it requires a very powerful sender to generate the weak authenticators, which will delay sending the packets. Additionally, weak authenticators will cause communication and computation overhead.

The Denial-of-Message attack is an attack that targets broadcast messages and prevents the sensors from receiving them. Researchers in (McCune et al., 2005) presented a scheme called Secure Implicit Sampling that increases the chances for a broadcasting base station to detect the failure of the sensors to receive its broadcasted message. A subset of nodes will send authenticated acknowledgments for each broadcasted message to the base station. The subset is tunable, thus unpredictable for an attacker. An obvious disadvantage of this scheme is the communication overhead resulted from the authenticated acknowledgments besides the requirement to use a special key for this task.

As discussed earlier, there is a high possibility in WSN for the nodes to be physically compromised, and thus all their secret information will be exposed. Aparnaa et al. (2019) discussed how a sensor node can get compromised and how to prevent these attacks in WSNs. (Alarifi & Du, 2006) proposed a technique to protect the secret keys of the sensors using diversity. Their scheme consists of two steps: at first, the data and the code of each sensor is obfuscated. This makes it difficult and time consuming for the attackers to find the secret data when they compromise a sensor node. Moreover, the scheme also requires that different nodes need to use different methods to obfuscate their data and codes. Consequently, the attackers cannot replace a node with another compromised one and also very hard to retrieve data from a large number of compromised nodes.

Time synchronization protocols provide a mechanism to synchronize the local clocks of the nodes in the WSN. Many protocols depend on the time synchronization between all the sensors in the WSNs, such as tracking and localization. Thus, it may be an attractive target for an attacker. Most of the protocols depend on the time-sensitive message exchange. An attacker may modify or forge time synchronization messages or even buffer and delay the messages and release them later to falsify the sensor's clocks. Wang et al. (2019) presented Tiny-Sync synchronization for WSN, in which they proposed an algorithm to analyze and enhance the performance of the time synchronization in WSN. Al-shaikhi et al. (2019) proposed an asynchronous protocol for WSNs, which they refer to as TSAU. This protocol mitigates the time synchronization errors and remains available even when the WSN is under attack.

7. Hardware Vs Software Cryptography

Another possible metric to classify broadcast authentication protocols in WSNs is the use of software versus hardware assistant to conduct the cryptographic operations. This classification is shown in figure 4. In the case where a hardware assistant is used, an external chip will be added to the sensor hardware. This approach has the advantage of not consuming the sensor's resources such as computations and storage but not the energy source. Nevertheless, it has two disadvantages. First, it lacks the flexibility to adjust the cryptographic algorithms, because it is difficult to modify and require replacing the chip with a new one. Second, it is critical to decide who will fabricate the cryptographic chips as they require a trusted party. It is not a good choice to leave it for the sensor’s manufacturers. On the other hand, using software assistant for the cryptographic algorithms will provide more flexibility and adaptability which makes it easier to adjust and modify the algorithms according to the choice of the designer. However, it may consume much of the sensor's limited resources such as computations and memory storage. Software codes can be written either on TinyOS using NesC or using the assembly language of the sensor’s processors. Using NesC has the advantage that it is easier to be implemented and can run on any sensor’s platform. Nonetheless, using the assembly language is much faster and efficient to run but is more difficult to write and modify. In addition, it has to be rewritten for different sensor’s platform.

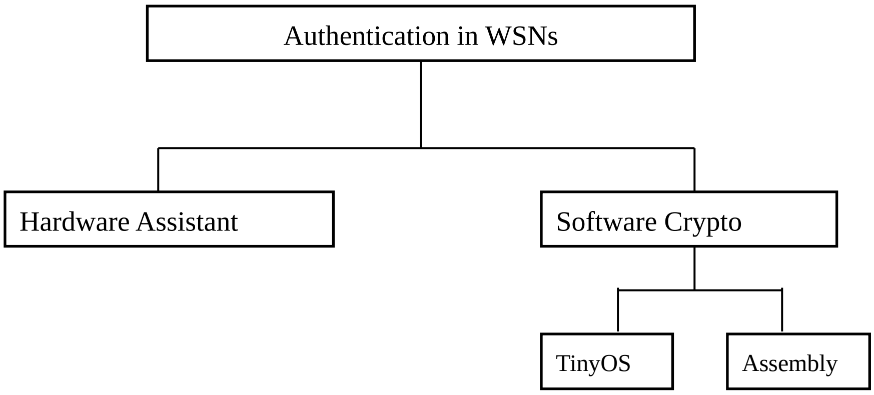

Figure 4. Classification of Broadcast Authentication

TinySec standard protocol used software assistant and was implemented to run on any sensor's platform that operates with TinyOS. Zigbee used hardware assistant and the cryptographic chips were appended to the sensor's hardware. Researchers in (Gaubatz et al., 2004) presented a hardware model for Rabin and NtruEncrypt and attempted to optimize the required size of the electronic chip's implementation.

Field-Programmable Gate Array (FPGA) is an embedded system that can be used as a hardware assistant to support authentication in WSNs. Researchers in (Mohd et al., 2016) proposed FPGA implementation to provide lightweight cipher algorithms to enhance security level. Toubal et al. (2020) proposed a field-programmable gate array (FPGA) circuit for a wireless sensor node to secure the transfer of data and key exchange.

8. Conclusions

With MCC, WBAN nodes will run the applications on remote rich servers located at medical facilities, and the nodes will be connecting the sensor/ actuator with the remote server through the 5G. Integrating 5G mobile networks with wMCC is a promising solution for the limitations in wMCC, in terms of providing a high level of QoS and performance. Moreover, 5G WBAN nodes can be deployed in larger numbers and have longer lifetime, all of which are critical for healthcare applications. Security is a critical issue for WBAN due to the sensitivity of their applications. Medical staff located on the cloud side usually send important commands to the actuator WBAN nodes to perform critical actions. The authenticity and integrity of these commands is the most critical security issue. Broadcast authentication is considered an open research area since none of the available protocols can fully satisfy all the metrics of the ideal protocol for broadcast authentication in WBAN/WSN. Protocols with a single MAC are not a good choice because they are vulnerable to node compromise attack, which is a common attack in WSNs. Due to the unreasonable large computational overhead multi-MAC and one-time signature protocols are both considered impractical for WSNs. µTESLA and ECC are the most practical protocols that can provide secure and reliable broadcast authentication in WSNs. The choice of which protocol to use is application dependent. If the application does not require immediate response and messages are sent frequently with predictable times, then µTESLA is considered a good choice. On the other hand, ECC can provide the best match with the seven metrics. In can be a secure and reliable choice for applications that require an instant response and send messages infrequently. Other public key protocols as Rabin, NtruEncrypt and RSA require large key sizes and high computational cost. The key sizes and the reasonable energy that ECC consumes makes it favorable compared to other protocols. Finally, we believe that this comprehensive survey and analysis for broadcast authentication in WSNs will help to select the best protocol for each application and motivate the researcher to design protocols that best work with their application.

References

Aborujilah, A., Nassr, R. M., Al-Hadhrami, T., Husen, M. N., Ali, N. A., Al-Othmani, A., ... Ochiai, H. (2019, September). Security Assessment Model to Analysis DOS Attacks in WSN. In *International Conference of Reliable Information and Communication Technology* (pp. 789-800). Springer, Cham. https://doi.org/10.1007/978-3-030-33582-3_74

Ahnn, J. H., & Potkonjak, M. (2013). mhealthmon: Toward energy-efficient and distributed mobile health monitoring using parallel offloading. *Journal of medical systems*, *37*(5), 9957. https://doi.org/10.1007/s10916-013-9957-0

Alarifi, A., & Du, W. (2006, October). Diversify sensor nodes to improve resilience against node compromise. In *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks* (pp. 101-112). https://doi.org/10.1145/1180345.1180359

Alhayajneh, A., Baccarini, A. N., Weiss, G. M., Hayajneh, T., & Farajidavar, A. (2018). Biometric authentication and verification for medical cyber physical systems. *Electronics, 7*(12), 436. https://doi.org/10.3390/electronics7120436

Almashaqbeh, G., Hayajneh, T., & Vasilakos, A. V. (2014, December). *A cloud-based interference-aware remote health monitoring system for non-hospitalized patients.* In 2014 IEEE Global Communications Conference (pp. 2436-2441). IEEE. https://doi.org/10.1109/GLOCOM.2014.7037173

Al-Shaikhi, A., Abdul-Rashid, R., & Masoud, A. (2019, March). Asynchronous Time Synchronization Protocol for WSNs. In *2019 16th International Multi-Conference on Systems, Signals & Devices (SSD)* (pp. 518-523). IEEE. https://doi.org/10.1109/SSD.2019.8893220

Aparnaa, M., Krishna, S. D., Amaran, S., Maheswari, S., & Soundarya, R. (2019, November). An Enhanced Scheme of Excluding Compromised Nodes in Wireless Sensor Networks. *Journal of Physics: Conference Series, 1362*(1), 012007. IOP Publishing. https://doi.org/10.1088/1742-6596/1362/1/012007

Benzaid, C., Lounis, K., Al-Nemrat, A., Badache, N., & Alazab, M. (2016). Fast authentication in wireless sensor networks. *Future Generation Computer Systems, 55,* 362-375. https://doi.org/10.1016/j.future.2014.07.006

Braeken, A., Liyanage, M., Kumar, P., & Murphy, J. (2019). Novel 5G authentication protocol to improve the resistance against active attacks and malicious serving networks. *IEEE Access, 7,* 64040-64052. https://doi.org/10.1109/ACCESS.2019.2914941

Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. (2011). Body Area Networks: A Survey. *Mobile Networks and Applications, 16.* https://doi.org/10.1007/s11036-010-0260-8

Da Conceicao, R. M., Lobato, R. S., Manacero, A., Spolon, R., & Cavenaghi, M. A. (2017, June). μTESLA protocol in vehicular networks. In *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). Ieee. https://doi.org/10.23919/CISTI.2017.7975802

Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless communications and mobile computing, 13*(18), 1587-1611. https://doi.org/10.1002/wcm.1203

Djellouli, A. E. A., Abdi, M. K., & Kechar, B. (2020). Formal verification of a new authenticated and optimized version of AOMDV for WSN. *International Journal of Communication Systems,* e4275. https://doi.org/10.1002/dac.4275

Du, W., Wang, R., & Ning, P. (2005, May). An efficient scheme for authenticating public keys in sensor networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing* (pp. 58-67). https://doi.org/10.1145/1062689.1062698

Elson, J., Girod, L., & Estrin, D. (2002). Fine-grained network time synchronization using reference broadcasts. *ACM SIGOPS Operating Systems Review, 36*(SI), 147-163. https://doi.org/10.1145/844128.844143

Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. *Future generation computer systems, 29*(1), 84-106. https://doi.org/10.1016/j.future.2012.05.023

Fortino, G., Di Fatta, G., Pathan, M., & Vasilakos, A. V. (2014). Cloud-assisted body area networks: state-of-the-art and future challenges. *Wireless Networks, 20*(7), 1925-1938. https://doi.org/10.1007/s11276-014-0714-1

Gaubatz, G., Kaps, J. P., & Sunar, B. (2004, August). Public key cryptography in sensor networks—revisited. In *European Workshop on Security in Ad-Hoc and Sensor Networks* (pp. 2-18). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-30496-8_2

Hu, X., Liu, C., Liu, S., You, W., Li, Y., & Zhao, Y. (2019). A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security. *IEEE Access, 7,* 125424-125441. https://doi.org/10.1109/ACCESS.2019.2937997

Jones, R. W., & Katzis, K. (2018, April). 5G and wireless body area networks. In *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)* (pp. 373-378). IEEE. https://doi.org/10.1109/WCNCW.2018.8369035

Karaca, Y., Moonis, M., Zhang, Y. D., & Gezgez, C. (2019). Mobile cloud computing based stroke healthcare system. *International Journal of Information Management, 45,* 250-261. https://doi.org/10.1016/j.ijinfomgt.2018.09.012

Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2019). *A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions.* IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/COMST.2019.2933899

Lamport, L. (1979). *Constructing digital signatures from a one-way function* (Vol. 238). Technical Report CSL-98, SRI International.

Luk, M., Perrig, A., & Whillock, B. (2006, October). Seven cardinal properties of sensor network broadcast authentication. In *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks* (pp. 147-156). https://doi.org/10.1145/1180345.1180364

Lynggaard, P., & Skouby, K. E. (2015). Deploying 5G-technologies in smart city and smart home wireless sensor networks with interferences. *Wireless Personal Communications, 81*(4), 1399-1413. https://doi.org/10.1007/s11277-015-2480-5

McCann, J., Moore, M., & Lumb, D. (2020, January 17). *5G: everything you need to know.* Retrieved from https://www.techradar.com/news/what-is-5g-everything-you-need-to-know

McCune, J. M., Shi, E., Perrig, A., & Reiter, M. K. (2005, May). Detection of denial-of-message attacks on sensor network broadcasts. In *2005 IEEE Symposium on Security and Privacy (S&P'05)* (pp. 64-78). IEEE.

McKinley, J. (2020). *5 Medical Devices You Didn't Know Could Be Hacked.* Retrieved March 16, 2020, from https://www.rd.com/advice/hacked-medical-devices/

Mohd, B. J., Hayajneh, T., Khalaf, Z. A., & Ahmad Yousef, K. M. (2016). Modeling and optimization of the lightweight HIGHT block cipher design with FPGA implementation. *Security and Communication Networks, 9*(13), 2200-2216. https://doi.org/10.1002/sec.1479

Nayak, P., & Devulapalli, A. (2015). A fuzzy logic-based clustering algorithm for WSN to extend the network lifetime. *IEEE sensors journal, 16*(1), 137-144. https://doi.org/10.1109/JSEN.2015.2472970

Ning, P., Liu, A., & Du, W. (2008). Mitigating DoS attacks against broadcast authentication in wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN), 4*(1), 1-35. https://doi.org/10.1145/1325651.1325652

Patwary, M. N., Nawaz, S. J., Rahman, M. A., Sharma, S. K., Rashid, M. M., & Barnes, S. J. (2020). The Potential Short-and Long-Term Disruptions and Transformative Impacts of 5G and Beyond Wireless Networks: Lessons Learnt from the Development of a 5G Testbed Environment. *IEEE Access, 8,* 11352-11379. https://doi.org/10.1109/ACCESS.2020.2964673

Piotrowski, K., Langendoerfer, P., & Peter, S. (2006, October). How public key cryptography influences wireless sensor node lifetime. In *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks* (pp. 169-176). https://doi.org/10.1145/1180345.1180366

Rabin, M. O. (1978). Digitalized signatures. *Foundations of secure computation,* 155-168.

Rahimi, M. R., Ren, J., Liu, C. H., Vasilakos, A. V., & Venkatasubramanian, N. (2014). Mobile cloud computing: A survey, state of art and future directions. *Mobile Networks and Applications, 19*(2), 133-143. https://doi.org/10.1007/s11036-013-0477-4

Shin, S., & Kwon, T. (2018). Two-factor authenticated key agreement supporting unlinkability in 5G-integrated Wireless Sensor Networks. *IEEE Access, 6,* 11229-11241. https://doi.org/10.1109/ACCESS.2018.2796539

Tai, W. L., Chang, Y. F., & Li, W. H. (2017). An IoT notion–based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks. *Journal of Information Security and Applications, 34,* 133-141. https://doi.org/10.1016/j.jisa.2017.04.002

Toubal, A., Bengherbia, B., Zmirli, M. O., & Guessoum, A. (2020). FPGA implementation of a wireless sensor node with built-in security coprocessors for secured key exchange and data transfer. *Measurement, 153,* 107429. https://doi.org/10.1016/j.measurement.2019.107429

Wang, S., Shi, M., Li, D., & Du, T. (2019, July). A Survey of Time Synchronization Algorithms for Wireless Sensor Networks. In *2019 Chinese Control Conference (CCC)* (pp. 6392-6397). IEEE. https://doi.org/10.23919/ChiCC.2019.8866385

Wang, T., Hu, K., Yang, X., Zhang, G., & Wang, Y. (2019). A trust enhancement scheme for cluster-based wireless sensor networks. *The Journal of Supercomputing*, *75*(5), 2761-2788. https://doi.org/10.1007/s11227-018-2693-y

Zhang, A., & Lin, X. (2017). Security-aware and privacy-preserving D2D communications in 5G. *IEEE Network*, *31*(4), 70-77. https://doi.org/10.1109/MNET.2017.1600290

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), 583-592. https://doi.org/10.1016/j.future.2010.12.006