GNSS : Navigation message authentication TESLA

Mia Filić
University of Zagreb
Faculty of Science, Zagreb, Croatia
University of Ljubljana
Faculty of Computer and Information Science
Ljubljana, Slovenia

Abstract

In this paper, the focus is on cryptographic spoofing defence of GNSS navigation channels based on TESLA protocol. Firstly, we explain how does the GNSS works and find its vulnerabilities. After, we analyse spoofing attack and how they can be mitigated. Determining the critical components which are vulnerable the most, the cryptography based defence utilisation is analysed. TESLA, selected navigation message authentication cryptography based protocol is presented and explained. Finally, some considerations and possible improvements of the TESLA protocol are discussed.

1 Introduction

The usage of Global Navigation Satellite System (GNSS) is widespred. Many applications use GNSS to provide or maintain their services:

- Goods/Assets tracking,
- Road tolling,
- Connecting (money) transaction with position and time

[23, 11, 15].

In an attempt to connect object with it position at certain time, the information about the position and time must be reliable. Geolocation of the object is usually determined either using one of the GNSS systems (i.e. GPS) or using information from telecommunication stations to triangulate the approximate position. GNSS approach is more accurate and mostly used. The telecommunication station approach is used if the GNSS system fails or as augmentation. [26]

The increasing commercial usage of GNSS raises concerns about the GNSS information authentication. While military uses GNSS signals which are strongly authenticated, commercial users still use signals which are available to everyone to change or retransmit (meaconing). In 2001, the U.S. Department of Transportation published a report estimating the vulnerability of the U.S. transportation infrastructure due to disruption of civil GPS [5]. The report emphasised the threats of spoofing and meaconing attacks which motivated greater research of the mentioned attacks. That has led to a greater progress in anti-spoofing field. [20] [21]

In general, we distinguish two types of spoofing defences, cryptographic and non-cryptographic. Cryptographic ones rely on secret keys that encrypt or digitally sign components of the broadcast signals while non-cryptographic do not. Non-cryptographic spoofing defence systems involves inertial measurement units or other hardware, which exceed the cost, mass, or size constraints of a broad range of applications [13]. The cryptographic spoofing defence system is attractive because it gives significant protection against spoofing attacks relative to the additional cost and bulk required for implementation. But, only in combination, they are most powerful.

In this work, close examination of TESLA based cryptographic spoofing defence definition is provided.

2 Global Navigation Satellite System (GNSS)

The term of Global Navigation Satellite System refers to constellation of satellites broadcasting ranging signals and Navigation Messages (NA) By definition, the GNSS has global coverage.

Nowdays, there are several GNSSs. Mostly used is Global Positioning System (GPS). GPS is owned and operated by US military. It provides two levels of operability. While one is restricted to authorised(often military) users, the other is free of charge for every-

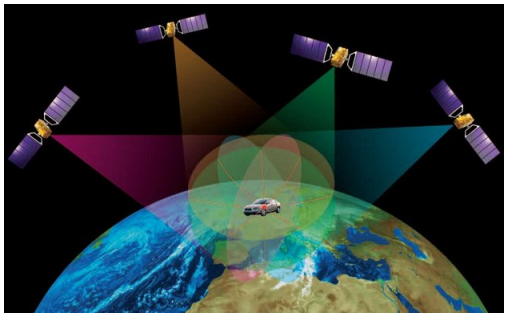

Figure 1: Satellite navigation [11]

one with the GPS-capable receiver. The second is Russia Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS). The third is Galileo, operated by European Union and scheduled to become full operable by 2020. [11] China is in process of expanding its regional BeiDou Navigation Satellite System into global one by 2020. [11] In following sections we will concentrate on the GPS system. If the information is related to some other GNSSs, that will be noted.

2.1 Navigation message

Each satellite provides data required for utilisation of the positioning determination process. The figure 4 shows the overview of content and structure of the satellite navigation message. [17]

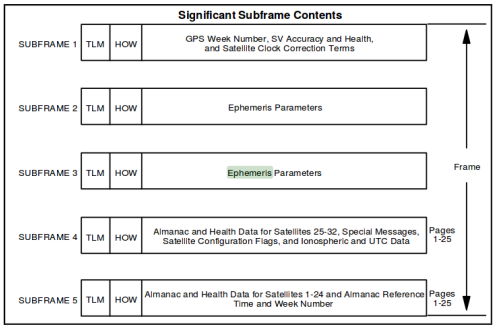

Figure 2: Navigation Message Content and Format Overview - one frame [17]

A Navigation Message is conducted of 25 frames. [11] One frame contains 5 sub-frames. Each frame contains information about the satellite system time when the next frame is transmitted. Each sub-frame needs 6s to be fully transmitted. The receiver is potentially capable of getting a new pseudo-range at the beginning of each sub-frame, or every 6 seconds. The pseudo-range is indirectly measured distance form transmitting satellite to the receiver.

For the purposes of this discussion, it is sufficient to understand that each navigation message is set of signals where each contains positioning and timing data (sending time, sender-satellite orbit, "satellite ID").

Figure 3: Navigation Message simplified

GPS and GLONASS detailed description of Navigation Message and positioning determination algorithm can be found in [11]. The same source contains detailed description of positioning determination process. General approach is described in next subsection.

2.2 Position determination process

As we mentioned before, each satellite transmits signals, Navigation Messages, which contains positioning and timing data. To determine receiver position, the latitude, longitude and height above the sea level need to be determined. Having 3 unknown parameters, there is need for at least 3 equations of full-rank system definition. [12]

The orbital data allows the receiver to calculate satellite position in Earth-Centered, Earth-Fixed X, Y, Z (ECEF XYZ) coordinates. [7]

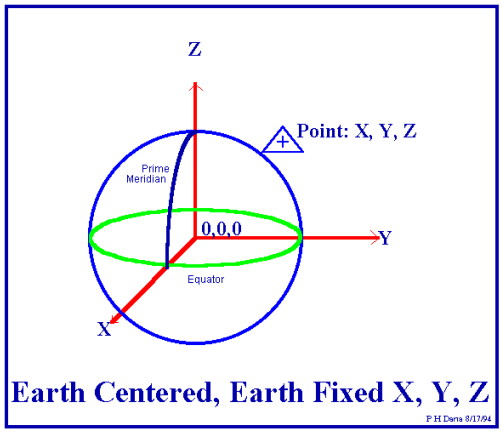

Figure 4: Earth-Centered, Earth-Fixed X, Y, Z (ECEF XYZ) coordinates [7]

Each receiver has a clock which enable calculation of

the signal, navigation message, receive time t'. Measuring the distance between GPS receiver and a satellite requires measuring the time it takes for the signal to travel from the satellite to the receiver. As the signal, transmitted by satellite i, contains "sending time" t_i, this can be computed as $(t_i' - t_c)$[1]

Knowing the elapsed time, multiplying it with the speed of light, c, the receiver-satellite pseudo-ranges are following:

$$d_i = c \times (t_i' - t_i)$$

as the satellite signals travel at the speed of light, approximately 300 000km per second.

Correct determination requires or the receiver time/clock to be synchronized with the satellite system time/clock as the forth unknown d_t. The pseudo-ranges equation is then following:

$$d_i = c * (t_i' - t_i + d_t)$$

Let $(x_i, y_i, z_i), i \in \{1,2,3,4\}$ be the positions of 4 different satellites and (x, y, z) the unknown receiver position expressed in ECEF coordinates.

The following equations in respect to x, y, z and d_t need to be solved:

$$d_1 = c * (t_1' - t_1 + d_t) = \sqrt{(x - x_1)^2 + (y - y_1)^2 + (z - z_1)^2}$$

$$d_2 = c * (t_2' - t_2 + d_t) = \sqrt{(x - x_2)^2 + (y - y_2)^2 + (z - z_2)^2}$$

$$d_3 = c * (t_3' - t_3 + d_t) = \sqrt{(x - x_3)^2 + (y - y_3)^2 + (z - z_3)^2}$$

$$d_4 = c * (t_4' - t_4 + d_t) = \sqrt{(x - x_4)^2 + (y - y_4)^2 + (z - z_4)^2}$$

As we can observe, at least 4 visible satellites need to be visible [2]. Visible satellite S by the receiver R at time T is every satellite from which R, at time T, can measure the signal propagation time (i.e. determine the pseudo-range) ant derive the corresponding valid equation

$$d_s = c * (t_s' - t_s + d_t) = \sqrt{(x - x_s)^2 + (y - y_s)^2 + (z - z_s)^2}$$

which can be used in positioning determination process.

After solving the system of equations, the (x, y, z) coordinates in ECEF system are estimated. Each receiver has an ability to transform ECEF coordinates into geodetic latitude, longitude and height above the Earth.

[1] More precise, travelling time is actually calculated by aligning pseudocode sequences (PRN codes). Both the satellite and GPS receiver generate the same pseudocode at the same time. The satellite transmits the pseudocode which is received by the GPS receiver. The receiver is still producing the pseudocode while the satellite's code is travelling. Eventually, the 2 signals are compared. The difference between the 2 signals is the travel time.

[2] In practice, even larger number of satellites is used to improve the accuracy of positioning determination process.

2.3 Vulnerabilities

As it was mentioned in the introduction, there are growing number of applications which utilise and rely on GNSS. The vulnerabilities of the GNSS becomes their vulnerabilities as well.

malevolent attacks on GNSS are roughly divided into the following three groups.

2.3.1 Jamming

Jamming in GPS means masking the satellite transmissions with strong local artificial signals affecting or even preventing the original satellite signal reception. [9]

2.3.2 Spoofing

Spoofing in GNSS involves transmission of signals of greater strength and mimicking the attributes of an original GNSS signal, thus taking over a GNSS. receiver.

2.3.3 Meaconing

Meaconing can be considered as one type of spoofing as it the interception and rebroadcast of navigation signals (meacon = m(islead)+(b)eacon. [14]

Figure 5: Spoofing in history: Pirates faking light-tower signals to lure cargo ships into dangerous waters and steal cargo from the wreck, "Mooncussers on rock with lanter"; Brenda Z. Guiberson

2.4 Navigation message authentication

As said before, the focus of the paper is on cryptographic spoofing defence, which assures the authentication of the determined position. In order to provide the position accuracy, there is a need to protect procedure and data from which the position is derived. To determine position, position of satellites and pseudo-ranges need to be calculated. In order to improve position accuracy, there is a need to protect not only the content of the navigation message, but also the process of propagation time measurement. If the signal arrives as delayed, pseudo-ranges will be increased, thus causing the incorrect position estimation.

Cryptographic protocol TESLA tries to overcome this obstacle by setting the agreement with the receiver at the beginning of the each conversation. Each communication between satellite and receiver can contain one ore more conversations. One conversation is attached to one key chain generation (explained later). At the begining of the conversation, satellite provides the receiver with data about the starting time of the conversation and the time interval between the sequence of messages correlated to the conversation. The time interval between messages can change dynamically as well. In that case, each message need to be supplemented with the time difference from the following message. That way the order of the messages in the conversation is preserved. The term message refers to the content data/useful data sent as one unit (packet or similar) trough the communication channel.

In general, elapsed time between two messages is set to be constant. Now, if the time of the arrival want to be forged, the time of arrival of all messages in the conversation need to be forged (delayed) which is much more complex. To produce valid message sequence is hard because, at the beginning of the conversation, the first message sent by the satellite is signed by it private key which is hard to forge. Also, because of the TESLA protocol definition, one message from the message chain is even harder to forge as.

Authentication of the navigation message may include the authentication of the navigation message content and the time-of-arrival. Authentication of the navigation message content in TESLA is provided in the packet-by-packet. The packet can be just one frame, subframe, or the whole navigation message.

3 TESLA protocol

Simply deploying standard point-to-point authentication protocol, i.e. appending a message authentication code (MAC) to each packet, does not provide secure broadcast authentication. The problem is that any receiver with the secret key can impersonate the sender. To prevent such a attack, we look at asymmetric cryptography schemes, digital signatures. Such a scheme provides secure broadcast authentication, but has a considerable large time and bandwidth overhead. Another approach is to modulate asymmetric properties using only symmetric cryptography,more specifically message authentication codes (MACs), and delayed disclosure of keys by the sender. This scheme was discovered by Cheung [6] in the context of authenticating link state routing updates. Similar approach was used in the Guy Fawkes protocol for interactive unicast communication [19].

The Time-Efficient-State-Less-Authentication (TESLA) protocol enables all receivers to check the integrity and authenticate the source of the signal in multicast or broadcast data stream environment. TESLA is an efficient protocol with low communication and computation overhead, which tolerates packet loss. [22] It is based on loose time synchronisation between sender and receiver. Despite using symmetric cryptographic functions (MAC), TESLA achieves asymmetric properties due to delayed disclosure of keys by the sender.

TESLA is widely applicable, from broadcast authentication in sensor networks [1], to authentication of messages in ad hoc network routing protocols [27].

3.1 Essential Knowledge for TESLA Protocol

TESLA requires that receivers are loosly time synchronized with a sender. This section provide simple loosly time synchronisation protocol. Also, it introduces the basic concepts of the MACs, one-way chain function, digital signature to provide better understandance of the TESLA protocol.

3.1.1 Message Authentication Code - MAC

Message Authentication Code (MAC) is used in message authentication. The plain message to be sent is, in cryptography, called plaintext M. The cryptographically changed(encrypted)/appended message that will be actually sent by the sender is called chipertext C.

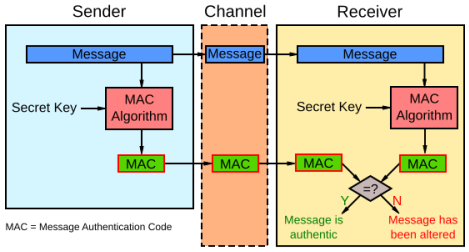

Figure 6: Message Authentication Code

As the goal of authentication is not to hide data, but to authenticate it, the chipertext C that the sender sends is simply the original message M together with a tag T, $C =< M,T >$. Tag T will provide the authentication of the message M. In cryptography, when the chipertext is of this form, we call communication mechanism a message-authentication scheme. Each message-authentication scheme is specified by the tag-generation(TG) algorithm and tag-verification(TF) algorithm. The tag-generation algorithm TG produces a tag $T \leftarrow TG(K,M)$ from a key K and the message. The tag-verification algorithm $B \leftarrow VF(K,C')$ produces a bit

from a key K, a message M', and a tag T'. With the intention that the bit B = 1 tells the receiver to accept M', while the bit B = 0 tells the receiver to reject M' as M != M'.

If the algorithm TG is stateless and deterministic, we call it, and the scheme itself, the Message Authentication Code (MAC). Also, in that MAC scheme TG = VG. MAC is keyed hash functions with some certain property relying on the secret key K, i.e. hash function with IV == K (secret key) It provides data integrity and the authentication of a message. One example of MAC is hash-MAC or HMAC which includes cryptographic hash function together with cryptographic key. To compute HMAC over the message m we perform

$$H(K \quad XOR \quad opad, H(K \quad XOR \quad ipad, m))$$

where
ipad = the byte 0x36 repeated B times,
opad = the byte 0x5C repeated B times.

The procedure folds as follows:

1. append zeros to the end of K to create a b byte string (e.g., if K is of length 20 bytes and b=64, then K will be appended with 44 zero bytes 0x00)
2. XOR (bitwise exclusive-OR) the b byte string computed in step (1) with ipad
3. append the stream of data 'm' to the b byte string resulting from step (2)
4. apply H to the stream generated in step (3)
5. XOR (bitwise exclusive-OR) the b byte string computed in step (1) with opad
6. append the H result from step (4) to the B byte string resulting from step (5)
7. apply H to the stream generated in step (6) and output the result

[18]

3.1.2 One-way chain

TESLA needs the effective mechanism operated within the receiver to authenticate MAC keys. For this purpose, it uses one-way chains. One-way chains are one of methods how to commit sequence of random values. One-way chains uses one-way hash function to generate a one-way chain.

The sender generates chain of size l by randomly selecting s_l and repeatedly applying the one-way function F to the s_l. We get sequence (chain): $s_l, s_{l-1}, ..., s_1, s_0$ where $s_i = F^{l-i}(s_l)$. Furthermore, $F^{i-j}(s_j) = s_i, j > i$ and $F^i(s_i) = s_0$ so every element of the chain can be verified having s_0 (self-verification). s_0 is called the commitment to the chain. The chain can either created at once and stored or each element can be calculated on demand having only s_l stored in advance. Usually, hybrid type is used to balance storage and computation overhead.

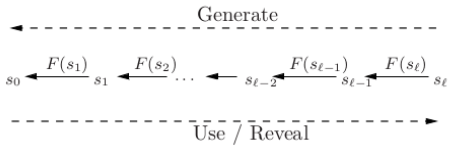

Figure 7: One way chain example. The sender generates this chain by randomly selecting sl and repeatedly applying the one-way function F . The sender then reveals the values in the opposite order. [22]

3.1.3 Loose time synchronisation

Loose time synchronisation between the receiver and sender means that receiver only needs to know upper bound on the sender's (satellite) local time. For the needs of TESLA, two-round time synchronisation is sufficient.

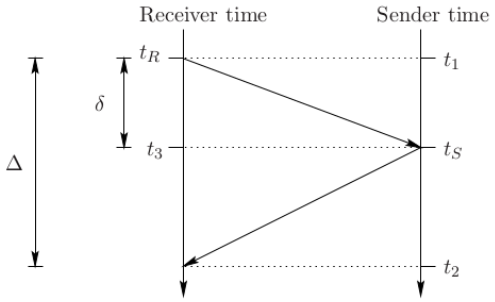

Figure 8: Direct time synchronisation between the sender and the receiver. [2]

Let δ be the real difference between the sender and the receiver's time. In loose time synchronisation, the receiver does not need to know the exact δ but only an upper bound on it, Δ

The protocol run as follows:

1. The receiver saves time t_r and sends the synchronisation request, Nonce to the sender.

2. By receiving the synchronisation request, the sender records time t_s, signs it together with Nonce and sends is back to the receiver.

3. The receiver verifies the digital signature and checks that the nonce in the packet equals the nonce it randomly generated. If the message is authentic, the receiver stores $t_R = t_r$ and $t_S = t_s$.

After the initial synchronisation, at any given time t, the upper bound on the sender time t_s can be calculated: $t_s = t_r - \delta \leq t_r - \Delta = t_r - t_R + t_S$.

Risk of denial-of- service attacks where an attacker floods the sender with time synchronisation requests, can be reduced aggregating multiple requests and signing it with the Merkle hash tree that is generated from all the requester's nonces. [16] which is sent to all the receivers. [2]

In GNSS application, Δ can be obtained from one of the positioning determination processes for which is considered to rely on authentic data.

3.2 Protocol

The main idea of TESLA is that the sender attaches to each message MAC computed with the key K known only to itself. The receiver buffers the packet, not being able to authenticate it. After a short while, agreed time interval, the sender reviles the key K. This way, one MAC per message, enable broadcast authentication.

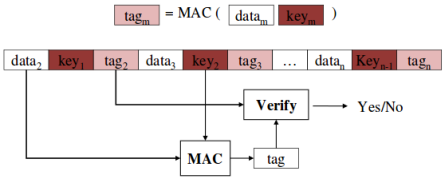

Figure 9: Overview of TESLA protocol

Protocol:

1. The sender determine N $\in N$, length of the key chain, limit on number of messages before the new one-way key chain need to be generated. Limit on the number of messages in one conversation. The sender generates random value for R_N. Using the one-way hash function, sender generates one-way chain of values $R_N, ..., R_1, R_0$.

2. The sender splits time into N time intervals of equal duration t_{int}: $t_0, t_1, ..., t_N$, To i-th time interval it attaches key R_i Observe that one-way chain is used in reverse order, so any key can be used to derive keys attached to previous intervals. The sender publishes the key R_i after the disclose time $i * L * t_{int}$. Disclosure time is often given in number of time interval between usage and disclose of the key, L.

3. Sender attaches the MAC to each massage m (i-th send message from the time t_0), where MAC of message m to be sent in interval $[t_i, t_{i+1})$ is calculated using key R_{i+1}. Along with the $MAC_m = MAC_{R_{i+1}}(m)$, sender attaches the most recent key that can be disclosed, $R_j, j = i + 1 - L$.

4. Each receiver that receives the extended message (MAC_m, m, R_j) does the following:

   - Check if the key used to compute the MAC is still secret by determining if the sender could not have yet reached the time interval for disclosing it. If the key is still secret, buffers the extended message.
   - Check if the disclosed key is correct using self-verification ($R_0 = F^j(R_j)$) and using previous keys.
   - Check the MAC of buffered extended messages which were sent in the interval $[t_{i-L}, t_{i+1-L})$. If the MAC is valid, the receiver accept messages.

Protocol steps are divided into 4 stages[22]:

- Sender Setup
- Bootstrapping receiver
- Broadcasting Authenticated Messages
- Authentication at Receiver

Steps one and two corresponds to "Sender Setup" stage, step three "Broadcasting Authenticated Messages" stage and step four "Authentication at Receiver" stage.

$$
\begin{aligned}
&t_0 : \mathsf{Sign}_{PK}(t_1, t_i - t_{i-1}, R_0), R_0 \text{ where } R_0 = h(R_1)\\
&t_1 : (\mathsf{Mac}_{R_2}(M_1), M_1, R_1) \text{ where } R_1 = h(R_2)\\
&t_2 : (\mathsf{Mac}_{R_3}(M_2), M_2, R_2) \text{ where } R_2 = h(R_3)\\
&t_3 : (\mathsf{Mac}_{R_4}(M_3), M_3, R_3) \text{ where } R_3 = h(R_4)\\
&t_4 : (\mathsf{Mac}_{R_5}(M_4), M_4, R_4) \text{ where } R_4 = h(R_5)\\
&\ldots
\end{aligned}
$$

Figure 10: Bootstrapping receiver(t_0) and Broadcasting Authenticated Messages with delay factor/disclose factor L equal to 1

In "Bootstraping receiver" stage receiver needs to be loosely time synchronized with the sender, know the disclosure schedule of keys, and receive an authenticated

key of the one- way key chain. It does not have to occur at time t_0. It can occur at any time, and starts with receiver synchronisation request. Response to the request, in general, contains following information:

- Time interval schedule: interval duration t_{int} , start time of current period t_i, index of interval i,length of one-way key chain.
- A key commitment to the one-way key chain R_j, where $max_j(j)$ ¡ i - d, the most recent key that can be disclosed. (d is the disclose offset in number of intervals)
- Disclose factor L

Before sending, the information is signed by sender's private key.

One-way chain has the property that if one of the intermediate keys (messages) are lost, the message can be authenticated by recomputing the lost key using later values. This makes TESLA packet lost resistant.

3.3 TESLA for Navigation Channels

In Navigation Channels, senders are satellites, and receivers GNSS receivers. Application of TESLA protocol in Navigation Channels does not require big additional cost and bulk required for implementation, but the format of Navigation Message need to be extended with MAC and corresponding hash key. Each satellite need to be attached to the hash function and private-public key pair for verifying and generating signatures in Bootstraping receiver" stage. Hash function can be the same for all satellites [10] or each can be attached to his own [4].

TESLA showed as a good tool for the geoencryption on Loran [25]. [8]

4 Discussion

4.1 TESLA security considerations

The security of TESLA relies on:

- The receiver's clock is time synchronized up to a maximum error of Δ.
- Function F is PRF(Pseudo random function), and F is weak collision resistant.

Until the above holds, it is computationally intractable for an attacker to forge a TESLA packet that the receivers will authenticate successfully [3]. Also, there is a need to have pseudo random function for generating R_N for each key chain generation. The pseudo random function can be the same for all satellites or each satellite can have its own. [3].

The cryptographic strength of the chain generation mechanism is significantly increased by breaking the symmetry of the iterations. This can be done by adding additional information to the hashing process that is known to the receiver, e.g., a counter or a time Tag. It is advisable to use this, modified, key chain generation mechanism. This way, if attacker somehow extract the sender hash-chain $s_o, ..., s_l$ from previous receiver-satellite communication, it can not reuse it, as it is was valid just for the certain period of time.

4.2 TESLA and Elliptic curves - a glitch

The problem with TESLA raises if the receiver has timing accuracy $\delta_r > T_i nt * d$, or greater than the time disclose offset. In such case, it does not prevent an attacker from replaying old data, or creating arbitrary message extension for creating valid packet. This can be overcome with hybrid approaches [4] , combining TESLA with Elliptic Curves cryptographic scheme, the signature scheme ECDSA. Due to [4] TESLA-ECDSA protocol achieves the best Navigation Message Authentication. The scheme drastically reduces overhead of verifying a digital signature in ECDAS while preserving cryptographic authentication of navigation data for all users, with arbitrary timing accuracy. The interested reader is advised to read the cited paper. Elliptic curves are one of the most used cryptographic oracles, so it is not strange at all to get across this kind of TESLA modification protocol.

5 Conclusion

The security of GNSS communication channels becomes more and more important. Increasing number of GNSS application, raises the global concern about it security, mostly implying the authentication. The paper discussed cryptographic based spoofing defence based on TESLA protocol. It gives full definition of the protocol and general utilisation in GNSS systems.

The TESLA protocol uses symmetric cryptography and achieves asymmetric property which is crucial for reliable broadcast message authentication. Used wisely, its utilisation can provide the high level of authentication security without significant change in physical

[3]The same PRN codes can have been used by several satellites at different points in time and a satellite may have used different PRN codes at different points in time. PRN codes are created by XORing 2 bit streams generated by linear feedback shift registers(LFSR) with maximal period 10. Different codes are obtained by delaying one of the bit streams. They repeat them self over time. Without the modification, the PRN generator can not be used as pseudo random number generator in key-chain construction.

model(architecture) of the system. Variety of applications [24, 1, 27] makes the protocol evolve. Each application of the TESLA protocol brings something new. If not more,a new security analysis is provided which is the base of protocol evolution and maintainability. Also, the protocol evolution, at most of the time, aims to increase the level of provided security.

References

[1] A. PERRIG, R. SZEWCZYK, V. W. D. C., AND TYGAR, J. D. Spins: Security proto- cols for sensor networks, 2001. In Proceedings of Seventh Annual International Conference on Mobile Computing and Networks (Mobicom 2001)[Online; accessed 2-Feb-2017].

[2] ADRIAN PERRIG, RAN CANETTI, D. S. J. D. T. Efficient and secure source authentication for multicast. https://users.ece.cmu.edu/~adrian/projects/tesla-ndss/ndss.pdf.

[3] ADRIAN PERRIG, RAN CANETTI, D. S. J. D. T. Efficient authentication and signing of multicast streams over lossy channels. https://people.eecs.berkeley.edu/~dawnsong/papers/tesla.pdf. [Online; accessed 4-Feb-2017].

[4] ANDREW J. KERNS, KYLE D. WESSON, T. E. H. A blueprint for civil gps navigation message authentication. [Online; accessed 2-Feb-2017].

[5] ANON. Vulnerability assessment of the transportation infrastructure relying on the global positioning system. *John A. Volpe National Transportation Systems Center, Tech. Rep.* (2001).

[6] CHEUNG., S. An efficient message authen- tication scheme for link state routing, 1997. In 13th Annual Computer Security Applications Conference, pages 90–98, 1997.

[7] DANA, P. H. Global positioning system overview. http://www.colorado.edu/geography/gcraft/notes/, 1994. [Online; accessed 9-Feb-2017].

[8] DI QIU, SHERMAN LO, P. E. D. B. Geo encryption using loran. https://web.stanford.edu/group/scpnt/gpslab/pubs/papers/Qiu_IONNTM_2007.pdf, 2007. [Online; accessed 4-Feb-2017].

[9] FERRARA, D. The definition of j/s jamming in gps. http://www.ehow.com/info_12212859_definition-j-s-jamming-gps.html. [Online; accessed 2-Feb-2017].

[10] IGNACIO FERNÁNDEZ-HERNÁNDEZ EUROPEAN COMMISSION, BELGIUM; VINCENT RIJMEN UNIVERSITY OF LEUVEN (KU LEUVEN), B. G. S.-G. U. A. D. B. S. J. S. E. G. A. C. R. I. R., AND CALLE, J. D. A navigation message authentication proposal for the galileo open service. *Journal of The Institute of Navigation* (2016). [Online; accessed 2-Feb-2017].

[11] J. SANZ SUBIRANA, J.M. JUAN ZORNOZA AND M. HERNÁNDEZ-PAJARES. *Fundamentals and Algorithms*, vol. 1. May 2013. [Online; accessed 9-Feb-2017].

[12] JIN, Z. Please explain full rank, definition. what it entails. http://www.cds.caltech.edu/~murray/courses/cds101/fa02/faq/02-10-28_fullrank.html, 2002. [Online; accessed 2-Feb-2017].

[13] KYLE WESSON, MARK ROTHLISBERGER, AND TODD HUMPHREYS. Practical cryptographic civil gps signal authentication. https://radionavlab.ae.utexas.edu/images/stories/files/papers/nma.pdf, Feb 2012. [Online; accessed 4-Feb-2017].

[14] LANGLEY, R. B. Innovation: Gnss spoofing detection. http://gpsworld.com/innovation-gnss-spoofing-detection-correlating-carrier-phase-with 2013. [Online; accessed 2-Feb-2017].

[15] MARTYN THOMAS. Global navigation space systems: reliance and vulnerabilities. http://www.raeng.org.uk/publications/reports/global-navigation-space-systems, 2011. [Online; accessed 9-Feb-2017].

[16] MERKLE., R. Protocols for public key cryptosystems, 1998. In 1980 IEEE Symposium on Security and Privacy , 1980.

[17] MILITARY, U. S. Global positioning system standard positioning service signal specification. http://www.gps.gov/technical/ps/1995-SPS-signal-specification.pdf, 1995. [Online; accessed 30-Jan-2017].

[18] NETWORK WORKING GROUP, I. Hmac: Keyed-hashing for message authentication. https://tools.ietf.org/html/rfc2104, 1997. [Online; accessed 2-Feb-2017].

[19] R. ANDERSON, F. BERGADANO, B. C. J. L. C. M., AND NEEDHAM, R. A new family of authentication protocols, 1998. ACM Operating Systems Review, 32(4):9–20, Oc- tober 1998.

[20] SCOTT, L. Anti-spoofing and authenticated signal architectures for civil navigation systems. In *Proceedings of the ION GNSS Meeting,Port- land, Oregon: Institute of Navigation* (2003), p. 1542–1552.

[21] SCOTT, L. Keeping the spoofs out: Signal authentication services for future gnss. In *Inside GNSS* (2011), vol. 6, p. 48–55.

[22] SONG, A. P. R. C. J. D. T. D. The tesla broadcast authentication protocol. https://people.eecs.berkeley.edu/~tygar/papers/TESLA_broadcast_authentication_protocol.pdf, 2002. [Online; accessed 2-Feb-2017].

[23] SUMIT S. DUKARE, DATTATRAY A. PATI, K. P. R. Vehicle Tracking, Monitoring and Alerting System: A Review. *International Journal of Computer Applications 119*, 10 (2015).

[24] SUWANNARATH, S. The tesla-alpha broadcast authentication protocol for building automation system. http://media.proquest.com/media/pq/classic/doc/4092454841/fmt/ai/rep/NPDF?_s=aVHQogcJ3K6hpQ3AJdvhVG5Kr48%3D, May 2016. [Online; accessed 4-Feb-2017].

[25] WIKIPEDIA. Loran. https://en.wikipedia.org/wiki/LORAN. [Online; accessed 4-Feb-2017].

[26] WIKIPEDIA. Geolocation, 2016. [Online; accessed 30-Jan-2017].

[27] Y.-C. HU, A. P., AND ARIADNE, D. B. J. A secure on-demand routing pro- tocol for ad hoc networks, 2002. In Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking (Mo- bicom 2002), September 2002.