International Journal of Trend in Scientific Research and Development (IJTSRD)

International Open Access Journal

ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Meaconing and Spoofing Attacks Evaluation with Enhancement in Security for Satellite Communication

Tarun Varma
Research Scholar, ECE, Mewar University,
Chittorgarh, Rajasthan, India

Dr. Akhilesh R. Upadhyay
Director, SIRTS, Bhopal,
Madhya Pradesh, India

ABSTRACT

Spoofing is the most dangerous threat of the ***GNSS*** infrastructure. Main goal of meaconing is to mislead the receivers tracking and sending wrong information about the signal position. The normal receiver is not conscious about this attack, and it acquires the counterfeit or mislead signal and discards the authentic signals. The rapid diffusion of *GNSS* location based applications which involve in large set of human activities makes the navigation system infrastructure very vulnerable against malicious attacks, which aim to disrupt the functionalities for illegal purposes. Considering into this scenario, efficient and computationally efficient detection and mitigation techniques are present in this paper in order to counteract spoofing and meaconing signals. The aim of this paper is to present possible and simple approaches in the spoofing detection field. Signal affected by spoofing signals are considered and detection methods are described pointing out the principal steps and possible applications, and drawbacks are also considered.

Keywords: *GNSS, Spoofing, Meaconing, GPS*

INTRODUCTION

The easy accessibility to the GNSS signal combined with a non security feature, as a cryptographic signature, in the signal modulation and data streams, makes civil infrastructures using open GNSS strongly vulnerable to jamming and spoofing attacks due to the predictability of open GNSS signals.[2] RFI is considered as the most disruptive event for the GNSS system. RFI affects the operation of the AGC and Low Noise Amplifier (LNA). Thus, due to the high possibility of such attacks, the GNSS security is a very important topic and consequently intentional interfering attacks are a serious threat for the overall navigation system, considering the rife diffusion in the daily human life applications as emergency and safety-of-life ones.[3] The attention is focused on the increasing risk of successful spoofing attacks due to the easy accessibility and cheap costs of the hardware and software equipment. If an attack is successful the navigation solutions are not reliable and the consequences are obvious, as misleading the navigation receiver[3]. Analyzing the effects on the GPS frequency signal, considerations that can be extended to other types of signals an navigation systems. Interference is a difficult threat for the GNSS infrastructure, and different type of jamming signal can be identified. Among them, the major issue is represented by the GNSS- like signals as meaconing and spoofing, as well. In order to define a meaconing attack, it is necessary to have a passive antenna which receives the useful signal, then an amplifier and a transmission antenna which works at the same GPS frequency of the useful signal[1][4]. All the receivers close to the jamming source detect the broadcast signal and decode the previous antenna position and not their own. It is possible to detect the presence of a meaconing attack if the rebroadcast signal has a higher power than the original signal. The spoofer was located close to the GPS receiver in order to acquire the signal .Along this way, a variety of wireless devices have been developed and deployed, some of them relying on human interaction (mobile phones, PDAs, navigation devices, etc.), others being mainly used for automated communication in networks of devices (sensor networks, mobile ad-hoc networks, satellite networks, etc.)[1][3][5].

How Spoofing attacks works

In spoofing attacks, the attacker aims to breach the integrity of wireless transmission while the receivers still receive messages and remain operational. On the one hand, spoofing may be an attack on the *sender integrity* and can result in identity. This can be achieved by eavesdropping wireless transmissions, extracting source information, and sending messages with forged sender data (insertion/injection attacks). On the other hand, spoofing can also be an attack on the *message integrity.*Typical examples of this are spoofing attacks on Global navigation satellite signals, in which the attacker modifies the data or sets any part of the data message to her liking.[6]To be precise, the integrity of wireless transmissions does not only relate to the data contained in the message and with that to sender and message integrity, which could be achieved by signatures. Integrity also refers to timing and power properties, i.e., to signal characteristics that cannot be protected by cryptographic primitives. To achieve such kinds of spoofing attacks that manipulate the timing or power properties, the attacker may *relay*or *replay* signals, or perform signal overshadowing attacks[7]. In *signal overshadowing* attacks, the receiver gets the attacker's signal and the original signal is discarded without the receiver noticing the replacement[8].

GPS Group Spoofing Attacks

We investigate spoofing attacks on GPS-based localization and time synchronization for single and multiple receivers and we analyze their feasibility and conditions for success. Spoofin refers to replay attacks and the insertion of crafted (self-composed) signals, but could also be achieved by the manipulation of legitimate signals during their transmission. GPS signals can be *(i) spoofed* to induce a wrong position or time at the receivers and *(ii) jammed* to prevent successful localization, navigation, and time synchronization at the receivers.

Effect of spoofing and Meaconing attacks on massages

Message Eavesdropping: The attacker can observe all messages sent to one or more receivers. In a wireless network, on the signal layer, an attacker can observe the channel and record all signals with own antennas. The interpretation of the received signals as messages may require secrets such as the used spreading codes, which might not be available to the attacker. In some scenarios, the attacker can be restricted in the number of channels that she can simultaneously monitor.[9]

Message Insertion and Replay: The attacker acts like a legitimate member of the network, and as such she can insert messages or replay previously received messages. In wireless networks, this is a reasonable assumption on both the message and signal layer because the attacker can construct own messages and transmit the corresponding signals and she can also replay previously received signals and messages. Restrictions on this can exist, e.g., in spread-spectrum communication using secret sequences shared between the sender and receivers[9].

Message Deletion: The attacker is in control of the network and can prevent the reception of messages. To achieve this effect on a wireless channel, several methods can be used on the signal layer. These methods include jamming of complete messages using higher energy noise signals as well as jamming only the message preamble to hide it from the receiver. A more covert attack is to annihilate the signal by sending inverse signals to the receiver. While these methods all have the same effect on the message layer, i.e., the deletion of the message, in each method the receiver will capture different signals on the (physical) signal layer.

Message Modification: The attacker can modify the messages obtained by the receivers. To modify wireless messages, the attacker can either change the signals during their transmission by adding own signals thus influencing the demodulation of single symbols by *symbol flipping*—or prevent the receiver from obtaining the original message (message deletion) and then insert a modified version of the message.

Attacks on unauthenticated (civilian) GPS

The attacker can delay signals or send them prematurely, they can modify the content of received GPS signals or arbitrarily generate the spoofing signals using the public GPS parameters (e.g., by using a GPS signal generator).[10] This is possible because civilian GPS signals are not authenticated and, given the right hardware, anyone can transmit own GPS signals. Thus the attacker can also modify the claimed locations of the satellites. On standard GPS receivers, the data content in the received GPS signals is not checked for plausibility or consistency[11].

Attacks on authenticated (military) GPS: The attacker is not able to generate valid GPS signals. All she can do is to capture and relay existing signals, e.g., by separating signals from different satellites using high-gain directional antennas and broadband transceivers (called *selective-delay*). This means that the attacker can delay existing GPS signals and amplify or attenuate them. Signals can be delayed but not sent prior to their reception. Here neither the spreading codes nor the data content of the signal need to be known to the attacker for successful selective-delay attack[11].

Spoofing Countermeasure Techniques

- Receiver Autonomous Integrity Monitoring (RAIM) method
- Consistency Cross Check with Other Navigation Systems
- Time of Arrival (TOA) Methods
- Navigation Message Analysis
- Correlation Peak Monitoring
- Spatial Discrimination of Spoofing Signals
- Power Based Method

The above first two methods are based on positioning, next two based on data bit and the last three are based on signal processing.[12][13]GPS spoofing detection based on lost, locks has two disadvantages: *(i)* strong attackers can achieve a seamless satellite-lock takeover, and *(ii)* lost, locks can also occur due to natural causes e.g., signal loss in tunnels or mountainous areas. GPS spoofing attacks that does *not* rely on the analysis of unusual signal characteristics or on the lost, lock of signals. Furthermore, it does not require any changes to the localization infrastructure or the satellites. The basic idea of this countermeasure is that, if the GPS receivers can exchange their individual GPS locations (e.g., using wired connections), they can check if their calculated locations preserve their physical formation within certain error bounds. In the case that the calculated GPS locations do not match the known formation, an attack must be suspected and there should be a warning. Even if only two GPS receivers are used, this countermeasure can detect any attacker that is using only a single antenna. In case of a single-antenna attack, the two GPS receivers would report the same location and could thus detect the attack.A strong attacker using multiple antennas could attempt to send signals such that the distances between multiple receivers are preserved. Nevertheless, each additional victim makes these spoofing attacks exceedingly more difficult because the space of possible antenna placements for the attacker gets significantly reduced. We know that there exists only one location per satellite where the attacker can place antenna this location is the rotated and translated satellite position of the GPS signal. Conducting such an attack is very difficult. It becomes even impossible if the receivers collaborate and can hide the exact position of at least one GPS receiver from the attacker e.g., by keeping it mobile on the vehicle, such that the attacker cannot adapt the sent signals to its position. In this paper we focused on signal processing technique.[14][15][3]

Spoof Detection Using Signal Strength Analysis

The spoofing nature of enemy effects on signal propagation and effect on signal strength stability due to calibration drift in wireless networking, this present significant challenges to using signal strength to detect wireless spoofs. The matching of sequence numbers is a non-trivial task because the generation of sequence numbers is a low-level device driver operation. Sequence number analysis for spoof detection is far from an exact science, the result is that most publicly available attack tools which involve a spoof do not bother attempt to match the sequence numbers of the target. The Sequence Number Rate Analysis (SNRA) technique calculates a “transmission rate” by taking the difference modulo. If the set of sequence numbers and arrival times suggests a transmission rate that is greater than the theoretical transmission limit, then SNRA concludes a spoof has occurred.[16][12]

Proposed Model of GNSS reciever

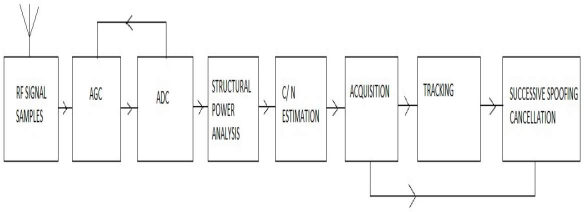
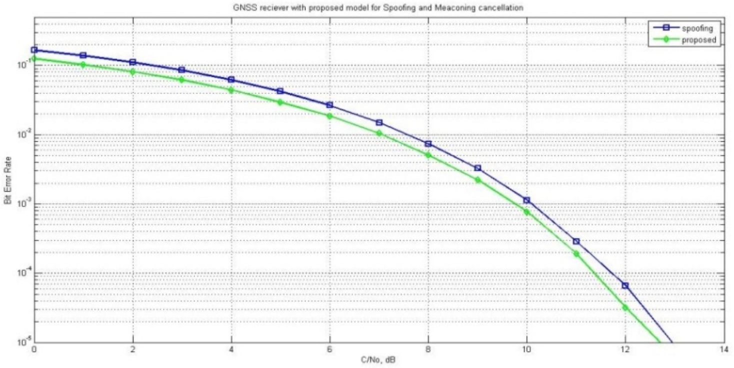


Fig.1 Proposed GNSS Reciever for Spoofing and Meaconing Cancellation

Simulation result



CONCLUSION

Proposed countermeasure in GNSS against GPS spoofing attacks requires no modifications of the GPS signal, the satellite infrastructure, or the GPS receivers, it is resistant against a wide range of attackers, and it can be deployed using multiple standard GPS receivers. We analyzed the requirements for successful GPS spoofing attacks on single victims and groups of victims with civilian or military GPS receivers. In particular, we identified from which locations and with which precision the attacker needs to generate signals in order to successfully spoof the receivers. When the group of victims grows in size, smaller numbers of spoofing locations become available until only a single point remains for five or more victims.

REFERENCES

1. 3rd Generation Partnership Project. 3rd generation mobile system. http://www. 3gpp•org.

2. ImadAad, Jean-Pierre Hubaux, and Edward W. Knightly. Denial of service resilience in ad hoc networks. In *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom),* pages 202-215, Philadelphia, PA, USA, 2004. ACM.

3. ImadAad, Jean-Pierre Hubaux, and Edward W. Knightly. Impact of denial of service attacks on ad hoc networks. *IEEE/ACM Transactions on Networking,* 16(4) :791- **802, 2008.**

4. Martin Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). In *IFIP International Conference on Theoretical Computer Science (IFIP TCS),* pages 3-22, 2000.

5. *David Adamy. EW101: A First Course in Electronic Warfare.Artech House, 2001.*

6. Dan Alistarh, Seth Gilbert, RachidGuerraoui, Zarko Milosevic, and Calvin Newport. Securing every bit: authenticated broadcast in radio networks. In *Proceedings of the 22nd ACM Symposium on Parallelism in Algorithms and Architectures (SPAA),* pages 50-59, Thira, Santorini, Greece, 2010. ACM.

7. ANSI. X9.63-2001: Key agreement and key transport using elliptical curve cryptography. Technical report, American National Standards Institute, 2001.

8. AnishArora and Lifeng Sang. Capabilities of low-power wireless jammers. In *IEEE InfoComMiniconference,* pages 2551-2555, Rio de Janeiro, Brazil, 2009.

9. Alfred Asterjadhi, Raju Kumar, Thomas F. La Porta, and Michele Zorzi. Broadcasting in multi channel wireless networks in the presence of adversaries. In *Proceedings of the Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON),* pages 377-385, Salt Lake City, UT, USA, 2011.

10. Baruch Awerbuch, Andrea Richa, and Christian Scheideler.A jamming-resistant MAC protocol for single-hop wireless networks. In *Proceedings of the ACM Symposium on Principles of Distributed Computing (PODC),* pages 45-54, Toronto, Canada, 2008. ACM.

11. ParamvirBahl and Venkata N. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom),* volume 2, pages 775-784, 2000.

12. Leemon C. Baird, William L. Bahn, Michael D. Collins, Martin C. Carlisle, and Sean C. Butler. Keyless jam resistance. In *Proceedings of the IEEE Information Assurance and Security Workshop (IAW),* pages 143-150, 2007.

13. Niko Bari and Birgit Pfitzmann. Collision-Free Accumulators and Fail-Stop Signature Schemes Without Trees. In *Advances in Cryptology EUROCRYPT,* volume 1233/1997 of *Lecture Notes in Computer Science,* pages 480-494. Springer Berlin / Heidelberg, 1997.

14. Elaine Barker and John Kelsey. Recommendation for random number generation using deterministic random bit generators (revised). NIST Special Publication 800- 90, NIST (National Institute of Standards and Technology), March 2007.

15. EmrahBayraktaroglu, Christopher King, Xin Liu, Guevara Noubir, Rajmohan Ra- jaraman, and BishalThapa. On the performance of IEEE 802.11 under jamming. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom),* pages 1265-1273, Phoenix, AZ, USA, 2008.

16. AlanBensky. *Wireless Positioning Technologies and Applications.* GNSS Technology and Applications Series. Artech House, 2008.

17. Bluetooth. Specification of the Bluetooth system (version 1.2), November 2003.

18. Stefan Brands and David Chaum. Distance-bounding protocols. In *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT),* pages 344-359, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.

19. Timothy X Brown, Jesse E. James, and AmitaSethi. Jamming and sensing of encrypted wireless ad hoc networks. In *Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc),* pages 120-130, Florence, Italy, 2006. ACM.

20. Antonio Cavaleri, Beatrice Motella, Marco Pini, and Maurizio Fantino. Detection of spoofed GPS signals at code and carrier tracking level. In *Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (Navitec),* 2010.

21. Yingying Chen, Wade Trappe, and Richard P. Martin. Detecting and localizing wireless spoofing attacks. In *Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON),* pages 193 -202, San Diego, California, 2007.

22. Jerry Chiang and Yih-Chun Hu. Dynamic jamming mitigation for wireless broadcast networks. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom),* pages 1211-1219, Phoenix, AZ, USA, 2008.