ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 342 - 346 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

Novel Techniques for Transmissions to Communication Jamming Denial-of-Service Attacks

[1]JOGI SUVARNA BHARATHA RAJU,[2] Dr. P. HARINI
[1]II year M. Tech[SE], SACET, Chirala , A.P.,anohu.anil@gmail.com
[2]Professor &HOD,Department of CSE, St.Ann's College of Engineering & Technology, Chirala, India.

Abstract:-A major challenge in securing wireless applications and services is the inherent vulnerability of radio transmissions to communication jamming Denial-of-Service (DoS) attacks. This vulnerability gains in significance the more one takes the ubiquity of these applications and services for granted and becomes a crucial factor in the context of safety-critical applications. At best, failures of safety-critical systems can result in substantial financial damage at worst, in loss of life. In this thesis, we investigate the fundamental primitives that enable jamming-resistant communication and propose novel anti-jamming techniques for scenarios where common anti-jamming techniques cannot be applied. This includes scenarios where network dynamics or lack of trust in the devices prohibits the pre-distribution of shared secrets (a prerequisite for common anti-jamming techniques), or where the use of anti-jamming communication is precluded by the constraints of the employed (e.g., narrowband and single-channel) transceivers. In the first part of this thesis, we tackle the problem of how devices that do not share any secrets can establish a jamming-resistant communication over a wireless radio channel in the presence of a communication jammer. We address the dependency between anti-jamming spread-spectrum communication and pre-shared keys that is inherent to this problem, and propose Uncoordinated Frequency Hopping (UFH), a novel anti-jamming technique, as a solution to break this dependency. We present and evaluate several UFH-based communication schemes and show their feasibility by means of a prototype implementation. In particular, we illustrate how UFH enables the jamming-resistant execution of (group) key agreement protocols in order to bootstrap common (coordinated) frequency hopping. In the second part of this thesis, we study the problem of jamming attacks on alarm forwarding in (security- and safety-critical) wireless sensor networks.

1. Introduction:

A major challenge in securing wireless applications and services is the inherent vulnerability of radio transmissions to communication jamming Denial-of-Service (DoS) attacks. This vulnerability gains in significance the more one takes the ubiquity of these applications and services for granted and becomes a crucial factor in the context of safety-critical applications. At best, failures of safety-critical systems can result in substantial financial damage—at worst, in loss of life. In this thesis, we investigate the fundamental primitives that enable jamming-resistant communication and propose novel anti-jamming techniques for scenarios where common anti-jamming techniques cannot be applied. This includes scenarios where network dynamics or lack of trust in the devices prohibits the pre-distribution of shared secrets (a prerequisite for common anti-jamming techniques), or where the use of anti-jamming communication is precluded by the constraints of the employed (e.g., narrowband and single-channel) transceivers. In the first part of this thesis, we tackle the problem of how devices that do not share any secrets can establish a jamming-resistant communication over a wireless radio channel in the presence of a communication jammer.

We address the dependency between anti-jamming spread-spectrum communication and pre-shared keys that is inherent to this problem, and propose Uncoordinated Frequency Hopping (UFH), a novel anti-jamming technique, as a solution to break this dependency. We present and evaluate several UFH-based communication schemes and show their feasibility by means of a prototype implementation. In particular, we illustrate how UFH enables the jamming-resistant execution of (group) key agreement protocols in order to bootstrap common (coordinated) frequency hopping. In the second part of this thesis, we study the problem of jamming attacks on alarm forwarding in (security- and safety-critical) wireless sensor networks. We argue that common anti-jamming techniques are beyond the capabilities of current sensor nodes and demonstrate the vulnerability to jamming of current forwarding schemes. Prompted by this deficiency, we discuss alternative jamming mitigation techniques and present a novel jamming detection scheme to counter advanced (reactive single bit) jamming attacks. We perform a detailed evaluation of the proposed schemes and validate our findings experimentally. The results show that our solution effectively detects sophisticated jamming attacks and enables the formation of robust sensor networks for the dependable delivery of alarms messages.

In this thesis, we investigate the fundamental primitives that enable jamming-resistant communication and propose novel anti-jamming techniques for scenarios where common techniques cannot be applied.

1.1 Jamming Countermeasures

In principle, there are three ways to counter communication jamming: jamming avoidance, jamming detection, and jamming mitigation. The arguably most evident and most effective way is to avoid the jammer by moving out of its range or by switching to a different communication medium (such as a wire) that is not affected by the jamming. But in spite of its effectiveness, avoiding the jammer is almost never possible: most wireless applications and services must be available at a specific location and entirely replacing the wireless communication infrastructure with a wired one is hardly ever a feasible option. The efficiency of jamming detection and localization as a means to counter jamming heavily depends on what the network entities can cause with the obtained information, that is, on whether effective and immediate countermeasures (e.g., the quick

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 342 - 346 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

deactivation/destruction of the jammer) can be taken. This de facto limits the application of jamming detection to settings where physical intervention is possible (and legal) or where no intermediate actions are required (i.e., where detection of the attacker is sufficient). The third and most common measure against jamming is to mitigate its impact by means of anti-jamming communication techniques that can resist the attack. Possible mitigation techniques include highly directional antennas, forward errorcorrecting codes, and spread-spectrum communication [5,60]. Common spread-spectrum anti-jamming communication such as frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS) enables the sender to spread a signal (in time and/or frequency) such that its transmission becomes unpredictable for the attacker. Provided that the attacker cannot physically isolate a device, her ability to alter or erase a message is restricted to interfering with the message transmission and is hence limited by the achieved processing gain of the spread-spectrum communication. The processing gain expresses the cost for the attacker to jam such a spread-spectrum transmission in terms of energy or power and is typically in the order of 100 to 1000 times the cost of the sender. The chances of success for such a malicious interference are thus in general sufficiently low—either because the attacker is not powerful enough to achieve more, or because she has no incentive to do so (e.g., if she wants to stay undetected).

1.2: Anti-jamming Communication without Shared Secrets

In the first part of this thesis, we address the problem of jamming-resistant communication in scenarios in which the communicating parties do not share secret keys. This includes scenarios where the parties are not known in advance or where not all parties can be trusted (e.g., jamming-resistant key establishment or anti-jamming broadcast to a large set of unknown receivers). An inherent challenge in solving this problem is that known anti-jamming communication techniques such as frequency hopping or direct-sequence spread spectrum require that the devices share a secret spreading key (or code) prior to the start of their communication. This requirement creates a circular dependency between anti-jamming spreadspectrum communication and key establishment and generally precludes the unanticipated anti-jamming communication between unpaired devices. As a solution to break this dependency, we propose Uncoordinated Frequency Hopping (UFH), a new spread-spectrum anti-jamming technique that does not rely on shared keys. We present and discuss several UFHbased anti-jamming communication schemes and show their usage for various applications, including the establishment of pairwise or group keys in order to bootstrap common coordinated frequency hopping. We thoroughly analyze the performance of our UFH communication schemes analytically and empirically via simulations. We identify an optimal strategy for theUFH frequency channel selection and show that, although it achieves lower communication throughput, UFH exhibits the same level of anti-jamming protection as common (coordinated) frequency hopping (which, however, cannot be used in scenarios where keys are not pre-shared). We further demonstrate the feasibility of our UFH schemes, in terms of execution time and resource requirements, with a software-radio-based prototype implementation.

1.3: Detection of Reactive Jamming in Sensor Networks

An integral part of most security- and safety-critical applications is a dependable and timely alarm notification. However, owing to the resource constraints of wireless sensor nodes (i.e., their limited power and spectral diversity), ensuring a timely and jamming-resistant delivery of alarm messages in applications that rely on wireless sensor networks is a challenging task. In order to demonstrate how challenging this task is, we present a state-of-the-art alarm forwarding scheme for wireless sensor networks that is fairly robust against unintentional link failures and investigate its resistance against jamming attacks. We show that in current alarm forwarding schemes blocking alarms by targeted, reactive jamming is not only straightforward, but that this jamming is also very likely to remain unnoticed by existing jamming detection schemes. In the second part of this thesis we address this problem and propose a novel jamming detection scheme for the identification of such targeted jamming attacks. Our scheme is unique in the sense that it is able to identify the cause of bit errors for individual packets by looking at the received signal strength during the reception of these bits and is well-suited for the protection of reactive alarm systems with very low network traffic. We present three different techniques for the identification of bit errors based on: predetermined knowledge, error-correcting codes, and limited node wiring. We perform a detailed evaluation of the proposed solution and validate our findings experimentally with Chipcon CC1000 radios. The results show that our solution effectively detects sophisticated jamming attacks that cannot be detected with existing techniques and enables the formation of robust sensor networks for the dependable delivery of alarm notifications. Our scheme also meets the high demands on the energy efficiency of reactive surveillance applications as it can operate without introducing additional wireless network traffic.

2. Anti-jamming Communication without Shared Secrets

A class of well-known countermeasures against communication jamming attacks are spread-spectrum techniques such as frequency hopping, direct-sequence spread spectrum, and chirp spread spectrum [60, 61]. Common to all these techniques is that they rely on secret (spreading) codes that are shared between the communication partners. These secret codes enable the sender to spread the signal (in time and/or frequency) such that its transmission becomes unpredictable for a third party, thus reducing the probability of interference. For these schemes to work, however, the required secret code must be shared between the partners prior to their communication, generally precluding (unanticipated) transmissions between unpaired devices or from a sender to an unknown set of receivers. The requirement of a shared code has so far been fulfilled by out-of-band code pre-distribution, which suffers from serious scalability problems. If pre-sharing the codes is not adequate or even infeasible (e.g., because not all communicating devices are known at the time of deployment or because the devices are not trusted to keep the keys secret) the devices must agree on a secret code (or key) in an ad-hoc manner using the wireless channel. However, the execution of a key-establishment protocol relies on jamming-resistant communication which, in turn, requires the availability of a shared secret code. In other

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 342 - 346 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

words, the dependency of spread-spectrum techniques on a shared key (or code) and the dependency of key establishment on jamming-resistant communication create a circular dependency, which we call anti-jamming/key-establishment dependency (see Figure 2.1). We point out that, even if the devices hold mutual publickey certificates issued by a commonly trusted authority, they still need to communicate in order to establish a secret spreading key (e.g., using an authenticated Diffie-Hellman key-establishment protocol) and to bootstrap common coordinated spread-spectrum communication.

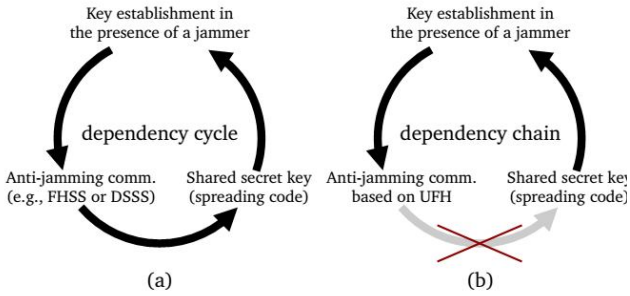

Figure 2.1: Anti-jamming/Key-establishment dependency graphs. (a) If two devices do not share any secret keys or codes and want to execute a key establishment protocol in the presence of a jammer, they have to use a jamming-resistant communication technique. However, known antijamming techniques such as frequency hopping and direct-sequence spread spectrum rely on secret (spreading) codes that are shared between the communication partners prior to the start of their communication. (b) In this work, we break this dependency and propose a novel frequency hopping scheme called Uncoordinated Frequency Hopping (UFH) that enables two parties to execute a key-establishment protocol in the presence of a jammer, even if the parties do not yet share a secret key or code.

In our present work, we break the dependency between anti-jamming spread-spectrum communication and shared secret keys. We propose a technique called Uncoordinated Frequency Hopping (UFH) that enables jamming-resistant (broadcast) communication without a pre-shared secret code. We present several UFH-based communication schemes that support the transmission of messages of arbitrary length and show how these schemes enable the execution of (group) key establishment protocols in the presence of a jammer. The established key can then be used by the communication parties to create a secret hopping sequence and to switch to more efficient coordinated frequency hopping for the subsequent communication. UFH is closely related to coordinated frequency hopping: each message is split into multiple parts and then sent across the air on random hopping frequencies chosen from a fixed frequency band. Like coordinated frequency hopping, UFH is based on the assumption that the attacker cannot jam all frequency channels on which the devices communicate at the same time so that the sender and receiver can still communicate through the remaining channels.

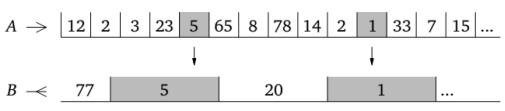

Figure 2.2: Example of UFH. The numbers indicate the frequency channels where sender A is sending and receiver B is listening over time (here, both send and receive on one frequency at a time). If A and B end and receive simultaneously on the same frequency (5 and 1 in the example), the packet sent on this frequency is successfully transmitted over the undisturbed channel.

However, unlike in common coordinated frequency hopping, in UFH, the sender and the receiver do not agree on a secret channel sequence but instead transmit and listen on randomly selected channels. Hence, all communication in UFH underlies the observation that, with sufficient transmission attempts, the sender and receiver will send and listen on the same channels in a number of time slots, even if they did not agree on them beforehand (see Figure 2.2). Intuitively, given 200 channels and given a sender hopping among the channels at a high rate of, for instance, 2 kHz, a receiver will be listening on the frequency where the sender is transmitting in average 2000/200 = 10 times per second (independent of the receiver's choice of the reception channels). Building on this observation, we develop UFH communication schemes that are highly resistant to packet losses, insertions, and active interference by an attacker. They can thus be applied in settings where users want to establish an unanticipated and spontaneous communication without pre-shared keys, which was so far not feasible using coordinated frequency hopping.

3: System and Attacker Model

We consider a scenario where a set of communication parties which do not share any secret values want to establish a jamming-resistant communication in the presence of a communication jammer. All parties reside within each other's transmission range and are equipped with a full-duplex radio transceiver capable of frequency hopping communication within a set C of $c = |C|$ frequency channels. The transceiver can be narrowband or broadband, enabling the parties to send and receive on one or more channels simultaneously; the number of channels on which the transceiver can send and receive on in parallel is denoted by c_t and c_r , respectively. We assume that the transceiver does not leak information about its active reception channels, that is, that the channels on which the transceiver is actively listening cannot be detected by monitoring its radio signal emissions. We further assume that a sender A splits its available transmission power uniformly over its c_t output channels such that it transmits with the same signal strength on all channels. With respect to a specific receiver B, we denote by P_A the strength of A's signal arriving at B and by P_A the minimal required signal strength at B such that B can successfully decode the signal (i.e., the sensitivity of B's receiver). In this context, a transmission between A and B over an undisturbed channel will be successful if $P_A >= P_t$ and if A sends on a channel on which B is currently listening. The parties share the same concept of time and their clocks are assumed to be loosely synchronized in the order of seconds (e.g., by means of GPS). Each party A is computationally capable of efficiently performing ECC-based public key cryptography and holds a public/private key pair (K_A ,K_A^{-1}), a corresponding public-key certificate A issued by a trusted Certification Authority (CA), and the valid public key K_{CA} of this CA. The keys and certificates were distributed during the system initialization phase (e.g., after the procurement of the devices) and the CA may be

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 342 - 346 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

off-line or unreachable at the time of communication. To increase the robustness of the message transmissions against interference and jamming, the parties apply error correcting codes with code rate r_c and resistance p to the messages.

3.1 Attacker Model

We consider an omnipresent but computationally bounded adversary that controls the communication channel in the sense that she is able to eavesdrop and insert arbitrary messages but can only modify transmitted messages by adding her own energy-limited signals to the channel. This means that the attacker's ability to alter or erase a message is restricted to interfering with the message transmission and that she cannot disable the communication channel by blocking the propagation of radio signals (e.g., by placing a device in a Faraday's cage). The attacker's goal is to interfere with the communication of the parties in order to prevent them from exchanging any useful information. That is, the attacker aims at increasing (possibly indefinitely) the time for the message exchange in the most efficient way. In order to achieve this goal, the attacker is not restricted to message jamming only, but can also try to disturb the parties' communication by modifying and inserting messages or by keeping the parties too busy to participate in or proceed with the protocol. More specifically, the attacker can choose among the following actions:

- The attacker can jam messages by transmitting signals that cause the original signal to become unreadable by the receiver. The portion of a message the attacker has to interfere with in such a manner depends on the used coding scheme.
- The attacker can modify messages by either flipping single message bits or by entirely overshadowing original messages. In the former case, the attacker superimposes a signal on the radio channel that converts one or several bits in the original message from zero to one or vice versa. In the latter, the attacker's signal is of such high power that it entirely covers the original signal at the receiver. As a result, the original signal is reduced to noise in the attacker's signal and the original message is replaced by the attacker's message. In either case, in this attack the signal must remain decodable by the receiver and result in a valid bit sequence.
- The attacker can insert messages that she generated by using known (cryptographic) functions and keys as well as by reusing (parts of) previously overheard messages (constituting a replay attack). Depending on the signal strength of the inserted messages, these messages might interfere with regular transmissions.

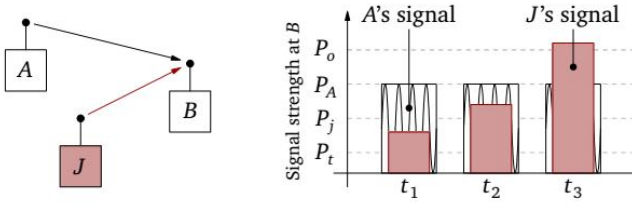

Figure 3.1: Required signal strengths for different attacker strategies. Let sender A transmit a message to receiver B such that the corresponding signal arrives at B with strength P_A. If an attacker J interferes using a signal that, at B, has lower strength than P_j, then B successfully receives A's message (t_1 in the figure); if, however, J 's signal arrives at B with a strength between P_j and P_o , the transmission is jammed, and B receives no message (t_2); finally, if the strength of J 's signal at B is even equal or greater than P_o it entirely overshadows A's transmission, and B receives J 's message (t_3).

4. Bootstrapping Coordinated FH with UFH-based Key Establishment

The bootstrapping of coordinated frequency hopping can be divided into two stages. In the first stage, the parties execute a key-establishment protocol and agree on a shared secret key K using UFH. Various keyestablishment protocols can be used in this step and we present the authenticated Diffie-Hellman protocol [7] and the Burmester-Desmedt protocol [17] as typical examples for two-party and group key agreement, respectively. Then, in the second stage, each party transforms the key K into a hopping sequence (using linear feedback shift registers and channel mappers [60]) and switches to coordinated frequency hopping. The first message in the second stage is typically a key confirmation that verifies the successful key agreement and, additionally, is used to synchronize the frequency hopping between the parties. Note that the established key is not used for encrypting or signing sensitive data but exclusively for generating the hopping sequence. Since our UFH communication schemes do not provide message authentication, all messages that are ex changed during the key establishment are signed in order to prevent the insertion of fake messages. In addition, the protocols use timestamps to preclude replay attacks and a (short-term).
history buffer to detect and drop duplicate messages during the validity of the timestamps. The period during which a message is considered valid is defined by the receiver and is usually in the order of time that is required to successfully transmit the message using UFH. Messages can be received more than once during their validity, either due to replay attacks or due to the repetitive message transmissions which are inherent to our UFH communication schemes. We point out that although an attacker may be able to replay an overheard message within the acceptable time interval in another protocol session, this does still not enable her to deduce the secret hopping sequence from it as the key contribution of the legitimate devices remains secret. In what follows, let G be an additive cyclic group of prime order p in which the Decision Diffie-Hellman (DDH) problem is hard and let P be a generator of this group. Because we are more concerned about minimizing the message sizes than the computational overhead, we assume that G is an elliptic curve group. Let further $\langle\rangle_X$ be the string in angle brackets concatenated with its signature by party X and let $\{\}_K$ be the encryption of the string in curly brackets with key K .

4.2 Anti-jamming Emergency Alerts

Two typical examples where a jamming-resistant dissemination of emergency alerts is required are (1) if a central (governmental) authority needs to inform the public about the threat of an imminent or ongoing (terrorist) attack while minimizing the risk that the attackers can jam the alert transmission, or (2) if a distress call in high sea operations (nautics) needs to be undertaken in face of an (imminent) adverse invasion (see Figure 7.3). Even under jamming, information dissemination in these settings is crucial. Being

able to disseminate the information within a delay (even of seconds) under jamming is clearly preferred over not being able to communicate any information at all.

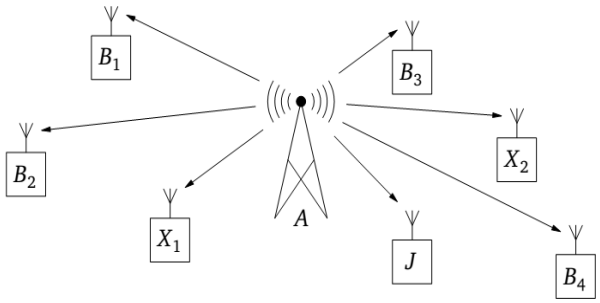

Figure 4.1: UFH-based emergency alert broadcast: Using UFH, a sender is able to disseminate a message to a set of unknown or untrusted receivers in an ad-hoc and jamming-resistant manner.

Once the information has been received by some entities, other communication means (e.g., speech or landline) may additionally support its dissemination to more people or authorities concerned. In addition to the single-hop broadcast scenarios given above, the antijamming emergency alert property of UFH communication can also be used for (multi-hop) jammer alarm forwarding in mobile ad-hoc or mesh networks. Jamming is a menacing threat to wireless networks because it deactivates the communication channel and thus, apart from disrupting normal network communication, also disables the transmission of jamming alerts and communication targeting to counteract the ongoing jamming. Here, UFH can be used for the delivery of short warning messages outside of the jammed region in an ad-hoc manner (i.e., without the need for any previous coordination among the nodes) from where external countermeasures can be taken.

5. Conclusion

We performed a detailed analysis of our UFH-based schemes and showed their feasibility by means of a prototype implementation. Our evaluation results show that even with our simple prototype, the average time to establish a pairwise or group key is in the order of a few seconds (for a processing gain of 23 dB). This time is reasonably short, given that the much shorter channel switching times and the higher data rates of purpose-built hardware allow to decrease this time significantly, and that with common anti-jamming techniques the devices would not be able to communicate and thus could not execute a key establishment protocol. We modeled and analyzed the impact of different attacker types and strategies on UFH communication and presented optimal channel selection strategies to counter these attacks. Our analysis also showed that, although our UFH scheme has lower communication throughput, it achieves the same level of anti-jamming protection as common frequency hopping.

References

[1] BTnodes – A Distributed Environment for Prototyping Ad Hoc Networks. ttp://www.btnode.ethz.ch/.
[2] GNU Radio Software. http://gnuradio.org/trac.
[3] ECRYPT Yearly Report on Algorithms and Keysize. D.SPA.28, July 2008. IST-2002-507932.
[4] ImadAad, Jean-Pierre Hubaux, and Edward W. Knightly. Denial of Service Resilience in Ad hoc Networks. In Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom), pages 202–215. ACM, 2004.
[5] David Adamy. A First Course in Electronic Warfare. Artech House, 2001.
[6] Özgür B. Akan and Ian F. Akyildiz. Event-to-sink Reliable Transport in Wireless Sensor Networks. IEEE/ACM Transaction on Networking, 13(5):1003–1016, 2005.
[7] ANSI. X9.63-2001: Key Agreement and Key Transport Using Elliptical Curve Cryptography. American National Standards Institute, 2001.
[8] International Loran Association. LORAN: LOng Range Aid to Navigation. http://www.loran.org.
[9] 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), pages 775–784. IEEE Communications Society, 2000.
[10] Leemon C. Baird, William L. Bahn, Michael D. Collins, Martin C. Carlisle, and Sean Butler. Keyless Jam Resistance. In Proceedings of the IEEE Information Assurance and Security Workshop (IAW), pages 143–150. IEEE, 2007.
[11] 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.
[12] Michael Baron. Probability and Statistics for Computer Scientists. Chapman & Hall/CRC, 2007.
[13] EmrahBayraktaroglu, Christopher King, Xin Liu, Guevara Noubir, RajmohanRajaraman, and BishalThapa. On the Performance of IEEE 802.11 under Jamming. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), pages 1265–1273. IEEE Communications Society, 2008.
[14] Josh Benaloh and Michael de Mare. One-Way Accumulators: A Decentralized Alternative to Digital Signatures. In Advances in Cryptology EUROCRYPT, volume 765/1994 of Lecture Notes in Computer Science, pages 274–285. Springer Berlin / Heidelberg, 1994.
[15] Alan Bensky. Wireless Positioning Technologies and Applications. Artech House, 2008.
[16] Dan Boneh, Ben Lynn, and HovavShacham. Short Signatures from the Weil Pairing. Journal of Cryptology, 17(4):297–319, 2004.
[17] Mike Burmester and YvoDesmedt. A Secure and Efficient Conference Key Distribution System. In Advances in Cryptology EUROCRYPT, volume 950 of Lecture Notes in Computer Science, pages 275–286. Springer Berlin / Heidelberg, 1995.
[18] Murat Çakiro˘ glu and Ahmet TuranÖzcerit. Jamming Detection Mechanisms for Wireless Sensor Networks. In Proceedings of the International Conference on Scalable Information Systems (InfoScale), pages 1–8. ICST, 2008.
[19] J.T. 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. IEEE Communications Society, 2008.
[20] Rohan Chitradurga and Ahmed Helmy. Analysis of Wired Short Cuts in Wireless Sensor Networks. In Proceedings of the IEEE/ACS International Conference on Pervasive Services (ICPS), pages 167–176. IEEE Computer Society, 2004.

AUTHORS:

JogiSuvarnaBharatha Rajucompleted B.tech in Computer Science &Engineering inChiralaEngineering college in the year of 2012 now pursuing M.tech in St.Ann's College of Engineering and Technology in Software Engineering(SE)

Dr. P. Hariniis presently working as a professor and HOD,Dept of Computer Science and Engineering,inSt.Ann's College of Engineering and Technology, Chirala.She obtained Ph.D in distributed and Mobile Computing from JNTUA, nanthapur. She Guided Many UG and PG Students. She has More than 18 Years of Excellence in Teaching and 2 Years of Industry Experience. She published more than 20 International Journals and 25 Research Oriented Papers in Various Areas. She was awarded **Certificate of Merit** by JNTUK, Kakinada on the University Formation Day on 21 - August - 2012.