A Wireless Sensor Networks Security Protocol Architecture

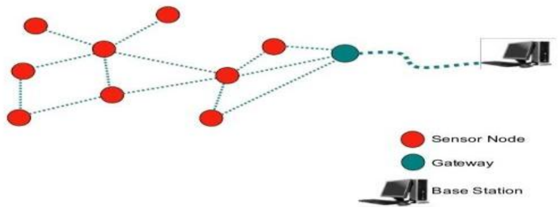
Parli B. Hari, Shailendra Narayan Singh

***Abstract**: A wireless sensor network is made up of extremely small autonomous units capable of sensing, computing and communicating. There are numerous restrictions on wireless sensor networks as the resource available to the wireless sensor network is limited. Thus, a number of clustering protocols in a routing sensor organization of sensor networks have been proposed in the literature which increase the throughput, save energy and decrease the delay in the system. In this paper, we put forward SNP, the one of its type link layer security architecture for wireless sensor networks. In this, the design vulnerabilities which were found in the protocols such as 802.11b and GSM are addressed using SNP. Security protocols have very conservative approach while guaranteeing the security and typically add up around 16-32 bytes as overhead. Owing to the scenario that sensor networks have limited supply of energy, little memory and low power processors, a 30 byte packet is more of unaffordable luxury for the wireless sensor networks. In SNP, the different trade-offs between separate cryptographic algorithms and wireless sensor network limitations are used to find an optimum point where packet overhead, security and resource requirements are met.*

***Keywords** : Wireless sensor network, Link Layer Security, MAC, Security, Design, SNP.*

I. INTRODUCTION

A wireless sensor network is made up of numerous sensor nodes having converging broader area connections as shown in Fig. 1. These find their use in numerous applications from non-overlapping applications which range from military uses to agricultural utilizations. The applications designed by using wireless sensor networks are usually missioned critical and thus make data security and data privacy as prime requirements. In wireless sensor network, achieving security is a challenging task as there is communication between different nodes makes it prone to a breach. Authentication and encryption need to go hand in hand through the transport node. However, there are constraints in terms of computational power, availability of energy. There is a significant enthusiasm over the utilization of wireless sensor networks. But there are a great number of limitations that come coupled with the wireless sensor network, one among them are the security of the network. As evident from Fig. 1, attacking a wireless sensor network is possible at numerous points. Thus, one of the biggest questions that arise is “securing a wireless sensor network” because without proper security mechanisms in place, extensive utilization of these networks would be truncated.



(Figure 1: Wireless Sensor Network)

To address the above said problem, SNP, a lightweight security architecture which can be easily integrated into the wireless sensor network application by developers is provided in this paper. Few research literature in the field of sensor networks dhow that around 50-80% all the 802.11 networks operate without any type crypto protection [1, 2, 3 and 4]. To accomplish a higher rate of utilization of sensor networks, the security scenario should be handy to use and must have minimal impact over the performance of the system. In a scenario, where any one among the previous is compromised, the developers will have sound good reason to leave out security.The design of SNP is over the prevailing security primitives which are proved by other researchers to be secure. Using these security primitives, we have designed an efficient as well as lightweight protocol that is specific to the sensor networks. SNP is a complete solution which defines the packet format, application interface as well as a thorough performance description. One of the biggest road blocks in adding security over a sensor network is their limited computation as well as limited communication capacities. As a matter of fact, security algorithms are not free; there are a lot of non-trivial performance issues while incorporating cryptographic algorithms. Even these limitations of sensor networks can be used for designing protocols which can ease the pain. For example, the bandwidth of the channel used in sensor networks is significantly less when compared to conventional networks. This signifies that even the most powerful network is limited in its packet per second transmission

Revised Manuscript Received on December 08, 2019

Parli B. Hari*, Research Scholar, dept of CSE, ASET, Amity University, Noida (UP), India.
Dr. Shailendra Narayan Singh, dept of CSE, ASET, Amity University, Noida (UP), India.

rate. Protocols design that depends upon properties like these is one among many strategies which are used to reduce the overhead. The design strategies used in this study of sensor network realizes the capabilities and limitations of these networks.

The main contributions of this paper are:

1. Introduction of SNP, one of its type protocol for cryptography in link-layer.
2. Explore some of the trade-offs among the wireless sensor networks.
3. Provide a cryptography protocol that suits the need of a wireless sensor network.
4. Test the implementation of SNP over a wireless sensor network.

II. SENSOR NETWORK

The term wireless sensor network is used for a heterogeneous system which can into existence by combining minute sensors and actuators through a general purpose computing hardware. A wireless sensor network can range from few nodes to thousands of wireless nodes. These networks are used in applications like habitat monitoring [5, 6 and 7], alarm systems, emergency response, war field surveillance and allied fields. A sensor node in our case was depicted by Mica2 as shown in fig. 2, Mica 2 happens to be a few inch big unit comprising of sensor as well as actuator unit which have CPU, power source, radio and other optional sensing elements. It has an 8-bit 8 MHz Atmel ATMEGA128L core with a 4 kB RAM, 512 kB flash memory as well as a low-powered radio manufactured by Chipcon which can be used over a single channel to deliver a 19.2 kbps bandwidth. Once fully charged, Mica2 can only be used for 2 weeks before running out of battery.

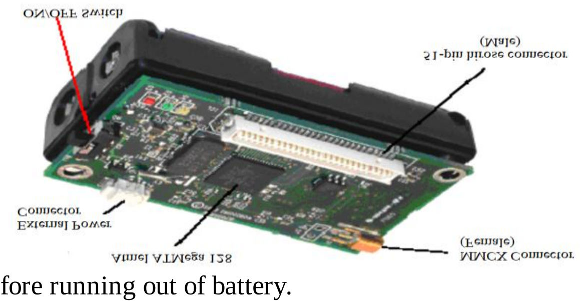


Figure 2: Mica2

It is clear from above discussion that sensor networks differ from distributed systems in many ways. A node in a sensor network has very little computational capacities. Thus, even the most resourceful public-key cryptographic algorithm must be used with care. Any deployed algorithm must also take into great acre the limited RAM and bandwidth capacity of the device. Even after taking care of these things, the energy consumption will remain a prime concern for the wireless sensor networks as that is very limited, too.

A. Vulnerability and attacks on a wireless sensor network:

Wireless sensor networks operate in a scenario which is altogether different from wired domain. Hence, are altogether different from the attacks in the later domain. All most all the wired networks benefit from their inherit security properties which are physical in nature. As evident from the case of physical nature, it becomes extremely unlikely that an enemy would come up and break the backbone of modern day internet. However, this is not applicable to the wireless communication networks as they are in broadcast medium by their inherit nature. When we are broadcasting, any opponent can easily come in and intercept/alter the data being transmitted. Also, any enemy coming in is not restricted to use sensor network hardware to intercept; they are free to use hardware of any type they wish to use. They can even interact with the hardware from ranged distance using radio frequency transmitters and high capacity workstations.Wireless sensor networks are also prone to attacks which are designed to consume the resource which is at the disposal of network. An attacker can send packets over and again which can consume all the battery with the sensors in a wireless sensor network and at the same time utilize the already limited bandwidth the network. As evident from the uses of a wireless sensor network, they can be deployed in varied environments. Thus, an enemy can even steal a node, recover their cryptographic material or even act as a part of the original network. However, in this paper, we are addressing all these threats. Our focus remains on authenticating the message. We are not considering other aspects of an attack in this paper.

B. Motivation

The security over a traditional network is maintained by using end-to-end mechanisms which include protocols like SSH [8], SSL [9] and allied. As evident from modern day technologies like whatsapp, the most predominant technology in market is end-to-end encryption as the medium just needs to read the header and it would be resource wastage for transmission medium to read the whole message. However, this is not the case with the sensor networks. In sensor networks, the most dominant message transfer pattern is many-to-one, where numerous sensor nodes communicate to one base station. One scenario which remains on top is that neighbouring sensor might be reading same environmental conditions and hence, multiple nodes may send same information to the base station. To overcome limitations of this type in-network processing was proposed which have techniques for duplication removal [10, 11]. Now, as evident from this scenario, in-network processing will require that the intermediate nodes have access to the message being carried. Thus, application of end-to-end encryption is viable option in this scenario. Also, end-to-end encryption is prone to attacks like denial-of-service. In case of end-to-end encryption, the integrity of message is checked at the final destination. Thus, there might be a scenario where the packets injected by the attacker have has passed through a number of hops before being detected. A link-layer based architecture has the capacity to detect the first instance where the packet has been injected in the network. Thus, a number of link-layer based mechanisms have been proposed in the domain of wireless sensor networks. For the reasons suggested above, it was decided to design SNP as a link-layer based architecture. This guarantees that the messages are authentic and confidential between the neighbouring nodes.

III. DESIGN OBJECTIVES

While designing SNP there were three major goals which are as follow

A. Security Objective

The basic requirement for any link layer protocol is to justify three properties: confidentiality, access control and integrity.

Confidentiality: As defined by the oxford English dictionary, confidentiality means the state of keeping or being kept secret or private. Thus, in case of wireless sensor networks, this means that the information is kept secret from unauthorized access. Usually, it is achieved by using encryption. In wireless sensor networks, a cryptographic technique should prevent an attacker from reading or accessing partial information being passed through message. It is known as semantic security [12] which implies that the attacker should not have more than a 50% chance of answering any encrypted message.

Access Control: Any protocol in the link layer should be in a position to prevent unauthorised entity from participating in the wireless sensor network. The nodes which are original in the network should be in a position to detect the messages which are from participants which are not a part of the original network and discard them.

Integrity: In addition to access control, the integrity of the message should also be preserved i.e. if an attacker changes a messages being transmitted and retransmits the same, then the original nodes in the network should be in position to recognise the same. SNP provides message authenticity by including a authentication code in the same.

B. Performance

The use of cryptographic techniques introduces an overhead in the messages. This produces a scenario where there is an increased demand in the domain of processing power, RAM utilization as well as the bandwidth. Latency and throughput have an inverse proportionality to the message length. Owing to all this, the sensor networks are also very sensitive to the power and an increased size will increase the power consumption as well. Thus, any architecture for cryptography is deemed to take care of all this.As evident from the discussion and the design of wireless sensor networks which have extreme resource scarcity, it becomes of critical importance that the security mechanisms are used in a fashion which provides necessary protection while handling the overhead issues.

C. Ease of Use

It can be expected that the security protocols which will deal with the higher levels will find link-layer based architecture as primitive and hence, use them as a component in them. Other difficulties in using the security protocols are that they are hard to implement and there are times when coders are not sure about the security parameters. This all makes it the concept of difficult to use specially in the case of wireless sensor networks.

IV. DESIGN OF SNP

A. Deficiency in Existing Schemes

Securing a channel which was previously not trusted by any member in the network has been extensively studied in the literature and there exist extremely huge amount of mechanisms to do so. Protocols like SSL/TLS, IPSec and SSH all perform extremely well in the internet communications domain. But the point of prime concern is that these protocols are extremely heavy to perform these tasks when utilized over a wireless sensor network. This happens mainly because of the reason that these were not originally designed to be utilized over a scenario with resource limitation.

Protocols which are somewhat close to the needs of a wireless sensor network were developed by communities belonging to mobile telephony and ad-hoc networking. Even these designs have extremely high amount of limitations when compared to the needs of a wireless sensor networks.

The result is that most of the schemes are not suitable for the wireless sensor networks as they are either insecure or consume too much of resource which is anyways a scarcity.

B. Design of SNP

A cryptographic protocol needs to have two parts in it. One part of it is the encryption part and the other being the authentication part, which in case of SNP is performed in a single go.

C. Encryption

Designing a secure encryption algorithm requires two major parts out of which one is encryption design and the other part is postulating the initialling vector format. In the design of SNP, we utilize a 12 byte initializing vector format and cypher block chaining. In this segment, the design of initializing vector for cypher bock chaining is discussed.

Cypher Block Chain: It is a method of using a cipher which is based upon blocks i.e. it contains a sequence of data which is encrypted in single block using a cipher/encryption key. It utilizes something which is known as the initialization vector (IV) of a particular length. An important characteristic of cipher block chain is that it implements a chain based mechanism that results in the decryption of a block being dependent on all the blocks which preceded it. Owing to this property, the validity of any block at nth location happens to be in the (n-1)th block. This results in a very interesting scenario where if there is an error of even a single bit, that will show an impact on the decryption of all the blocks that are preceding that block. If there happens to be a rearrangement in the blocks that would result in whole of process of decryption to become corrupt. Hence, would depict a possible attack.

SNP initializing vector (IV) format: The goal of this work is to decrease the cost of security in a wireless sensor network. Thus, the size of initialization vector (IV) and the mechanisms to generate the initialization vector can dramatically alter the performance of system. If the initialization vector is too lengthy, it would increase the bits which are added to the packet without any necessary bias. This would result in increasing the cost of implementation as well as decreasing the throughput and will drain the already limited power supply. Also, if initialization vector is too small then the chances that it would cause repetition increases which would compromise the security of whole of the wireless network.

The pigeonhole principle states that an initialization vector of length n will definitely repeat once 2^n+1 packet have been dispatched, irrespective of the length of the initialization vector. If we are using an n-bit counter to check for repetitions, it can be said with certainty that repetitions will not take before that point. However, it can also not be denied that in few strategies employed for generating initialization vector, repetitions can take place before that. If we utilize the birthday problem to deduce the initialization vector we find that chances of repetition come as early as $2^{n/2}$ packets. Thus, SNP uses an initialization vector which contains a counter in it and that counter is transmitted helping the receiver to identify the value of counter.

The design of initialization vector is D_add||AM||len||src||cnr, where D_add specifies the address of the destination, AM specifies the active message handler type, len specifies the length of message, src specifies the address of the source from where the message have been originated and cnr specifies the 32 bit counter. The counter starts with its initial value as 1 and is continuously incremented by 1 after each successful transmission.

D. Authentication

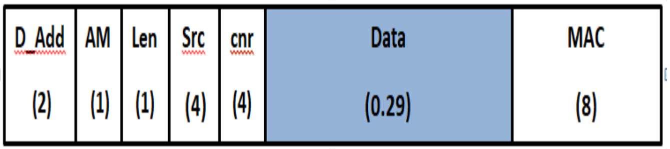
It has been pointed out in few under-consideration research literatures [13, 14, and 15] that employing encryption without utilizing any authentication mechanism is insecure. If there is not an authentication mechanism, the whole system is prone to copy-and-paste type attacks [13]. In these types of attacks, an attacker breaks the encrypted message and designs another encrypted message with something meaningful in it.

To overcome the above said vulnerabilities, SNP always encrypts and authenticates the messages. Message confidentiality is important components in a network were data is of prime concern. For example, the tsunami early warning systems, if an attacker triggers this system in a costal country there could be havoc and loss of precious man-hours coupled with panic. The actual content of the message would be just a signal being triggered mostly which is loud sound. If unauthenticated, it can be triggered with relative ease and even from unauthentic sources. However, today almost all applications need authentication. Thus the possibility of such a scenario is quite low.

SNP utilizes a block chain based cipher construction for calculating and verifying message authentication code. This is an efficient and computational viable methodology for authentication. Again as SNP is based upon the block cipher, thus the number of primitives already low and must be implemented in the limited memory we have. Cipher block chaining is usually secure except for the instance where it is used for a variable sized message.

E. Packet Format of SNP

The packet format for SNP is as depicted in the fig. 3. The fields which are common to the cipher block chaining are destination address (D_add), active message (AM) type and length



D_Add	AM	Len	Src	cnr	Data	MAC
(2)	(1)	(1)	(4)	(4)	(0.29)	(8)

Figure 3: SNP packet format. The byte size of each field is indicated below the label.

(len). The active message types are somewhat similar to the port numbers which are used in the TCP/IP. The active message (AM) type block states the suitable type of hander function which can be used to retrieve and decipher the message at the end of the receiver. These fields are intentionally unencrypted as the benefit of sending it unencrypted outweighs the benefits of sending them with encryption as the resources are already constrained in the wireless sensor network. This technique of sending messages can come handy to save power, like in the scenario a node detects that a message is meant for that particular node thereby it can switch off its receiver to save power. A sensor network employs broadcast as its medium of communication, thus nodes can utilize early detection at the AM head its self and save precious power. If we encrypt the address and AM head, it will become impossible for any node to perform early detection until the nodes had deciphered the contents. This would result in power consumption without any meaningful output. Also, the length of any message can be found regardless the encryption of the length field. To find out any transmission error, a cycle redundancy check is performed in most of systems. In it, receiver computes cycle redundancy check once a packet is received and crosses-validates it against the cycle redundancy check head received with the packet. If the head matches with the cycle redundancy check value, then the receiver accepts the package or else rejects the package. One broader limitation of cycle redundancy check is that they are ineffective in providing any authentication against the malicious alterations of the packets being sent. To provide authentication against malicious alterations in the packets SNP utilizes the message authentication code (MAC) as against cycle redundancy check. The message authentication code provides protection to the whole packet starting from destination address to the last point of data, whether encrypted or not. This helps to safeguard data from tempering. This way it also arrests any move from any attacker who may be redirecting the packages, stop the truncation of packets and limit all other type of events. Message authentication protocol has an inherit capacity of detecting any alteration in the data; hence the slightest need for a cycle redundancy check is also removed.

V. RESULTS

A. Measurements

It is very clear from the above design that SNP increase the implementation costs in terms of computational power thereby increasing the energy requirements. For the purpose of development the load which is provided by the implementation of SNP must be substituted by a higher benefit costs or else development process won't utilize the protocol, if it provides higher implementation costs and lower benefits. In SNP, there happens to be two main components which add to these implementation costs. These components are:

a. The size of packet is higher when using SNP as compared to the size of packet when SNP is not utilized

b. Requirement of a higher computational power as a result of increased packet size. This results in higher time of computation as well as increased energy consumption.

To compute the cost of implementing cryptography using SNP, the effect which is introduced by the length of SNP's packet in a wireless sensor network? It is clear from the previous design as discussed in section 4 that SNP increases the length by 8 bytes. Longer packets increase the implementation costs in the following ways:

a. The increase the bandwidth utilization. Thus, decrease the effective bandwidth available in the wireless sensor network.

b. Introduction of SNP would increase the latency owing the slow communication channels.

c. SNP increases the packet size. To transmit an increased packet size the transmission radio must stay active for a longer period. Thus, increases its energy consumption.

For providing an analytical overview of SNP, we first provide the contribution expected solely from transmitting the increased packets. Table 1 depicts the increase in latency caused by the introduction of SNP into a wireless sensor network. An increase of 12% most can be expected to be introduced into the system by SNP. It is important to mention here that transmitting a packet is more than just transmitting the data and header for same; since we incorporate message authentication code, a 28 byte start symbol as well as additional synchronization bytes are transmitted as well. This brings down the influence of embedding extra byte of overhead because of high fixed cost for transmitting a packet.

Table 1: Increase in latency caused by SNP

	Data	Overhead per packet	Total size (a+b)	Transmission time (ms)	Percentage Increase in latency
Without – SNP	48	36	84	38.2	
With - SNP	48	44	92	42.7	12.09%

The implementation of SNP over Mica2 was performed and its performance was measured experimentally for the changes it gave in terms of bandwidth utilization, energy consumption and latency in the network. The evaluation has been done over a number of micro-benchmarks.

Cipher Performance: Performance of two block based ciphers namely RC5 and Skipjack was tested to deduce their speeds. Any system implementing a lock cipher operation must be in a position to complete it with extremely high speeds due to the overlapping of radio operations. Also, if a cipher will execute in extremely high speeds, it will consume less energy.

The results for the comparison between RC5 and skipjack are provided in table 2 and it can be seen that both are quite good choice as far as their utilization in link-layer is concerned. Also, each operation is of 8 bytes with a time frame of maximum 0.95 ms, thus there are ciphers are quite very fast. As a matter of fact, block cypher operation should get executed within few micro-seconds, if it doesn't happens on then the radio must be kept on for longer time. Hence, would result in drain of power. It should be noted in table 2 that RC5 has 2 versions because of the reason that the initial code was enhanced in its inner loops to increase its performance whereas same was not done with skipjack. It is important to mention here that increasing the performance of skipjack is possible if the internal looping structure is adjusted to suit the requirements.

Table 2: cipher execution time

Cipher	Time (ms)
RC5 – unedited	0.95
Skipjack	0.4
RC5 - edited	0.29

Energy consumption: To figure out the amount of energy drawn using SNP, the concept of instantaneous current was utilized. A sample of 48 bytes of application data was sent and the amount of instantaneous current withdrawn by the transmitter was measured. The radio was exposed to byte level interface.

It was found out in the measurements that large current was withdrawn at the start of operation because of the cryptographic operations. When the transmission process starts, SNP was having overlapping in encryption and message authentication code part with the sending of start symbol. The start symbol happens to be of 16 bytes. For the largest size packet to be sent across 10 cipher operations were required, thus the block cipher must not take 16/10 = 1.6 byte times per operation. This depicts that the block cipher consumes processing power heavily which results in a large initial withdrawal of power.

Throughput: To determine the maximum amount of throughput while using SNP, we computed the number of packets that we were able to send in 1 minute time frame. For this, we organized a number of mica2 sensors in form of a network in such a fashion that various nodes would transmit at the same time. The number of senders had a direct proportionality to the utilization of the channel. Thus, number of senders was altered. This alteration made way for characterization of throughput at different utilization frames. In this study it was observed that the SNP had an 8% less throughput as compared to the scenario when this technique was not utilised. One observation which is of prime concern here is that when there are few senders in the network, the throughput was not of major concern as it was anyways at lower end. The results are shown in figure 5. In figure 5, x-axis represents the number of hops and y-axis represents the route time (ms).

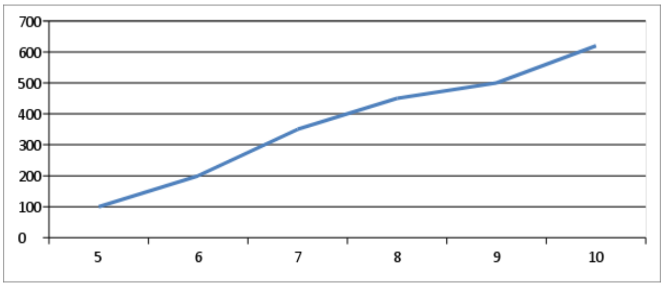


Figure 5: Latency chart

VI. CONCLUSION

There are number of devices especially in the field of wireless sensor networks where energy and processing power are the major limitations. SNP is a viable architecture to be used over that. SNP has been designed to handle scenarios like these and designed over the existing security protocols. The highlights of the design process are highlighted in the research paper from a cryptographic point of view which happens to meets the resource constraint scenario. In SNP, we are utilizing the cryptographic primitives which have been used in the community for quite some time now.

The performance of the architecture had been presented throughout the paper. It just increases the energy consumption of the total system by a minute amount 12% when used in its most resource utilizing way. Also, it was also observed that the impact on latency and bandwidth was quite low. Hence, it is very viable to utilize this architecture in any of the wireless sensor network.

REFERENCES

1. Chris Hurley. The worldwide wardrive: The myths, the misconceptions, the truth, the future. In Defcon 11, August 2003.
2. Peter Shipley. Open WLANs: the early results of wardriving, 2001.
3. Mohamed G. Gouda, E.N. Elnozahy, Chin-Tser Huang, and Tommy M. McGuire. Hop integrity in computer networks. IEEE/ACM Transactions on Networking, 10(3):308–319, June 2002.
4. WiGLE. Wireless geographic logging engine—general stats, December 2003.
5. Smart buildings admit their faults. Lab Notes: Research from the College of Engineering, UC Berkeley, http://www.coe.berkeley.edu/labnotes/ 1101smartbuildings.html, November 2001
6. Alan Mainwaring, Joseph Polastre, Robert Szewczyk, and David Culler. Wireless sensor networks for habitat monitoring. In First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.
7. Robert Szewczyk, Joseph Polastre, Alan Mainwaring, and David Culler. Lessons from a sensor network expedition. In First European Workshop on Wireless Sensor Networks (EWSN '04), January 2004.
8. T. Ylonen. SSH - secure login connections over the Internet. In Proceedings of the Sixth USENIX Security Symposium, 1996.
9. OpenSSL. http://www.openssl.org.
10. Samuel R. Madden, Michael J. Franklin, Joseph M. Hellerstein, and Wei Hong. TAG: A tiny aggregation service for ad-hoc sensor networks. In The Fifth Symposium on Operating Systems Design and Implementation (OSDI 2002), 2002
11. Samuel R. Madden, Robert Szewczyk, Michael J. Franklin, and David Culler. Supporting aggregate queries over ad-hoc wireless sensor networks. In Workshop on Mobile Computing and Systems Applications, 2002.

12. M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation. In Proceedings of 38th Annual Symposium on Foundations of Computer Science (FOCS 97), 1997.
13. Steven M. Bellovin. Problem areas for the IP security protocols. In Proceedings of the Sixth USENIX Security Symposium, 1996
14. Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting mobile communications: The insecurity of 802.11. In The Seventh Annual International Conference on Mobile Computing and Networking (MobiCom 2001), 2001
15. Hugo Krawczyk. The order of encryption and authentication for protecting communications (or: How secure is SSL?). In Advances in Cryptology – CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science. Springer-Verlag Heidelberg, January 2001

AUTHORS PROFILE

Parli B. Hari received his M.E. (Computer Science & Engineering) degree from Dr. Bhim Rao Ambedkar University, Agra (Formerly Agra University, Agra) in 2006 with Honors. He also qualified the UGC-NET in 2013. He started his teaching career from University campus of Dr. B. R. Ambedkar University, Agra from 2003. He taught B.Tech, M.Tech, MCA, MBA courses in various universities. He also published 15 research papers in repute journals and conferences at national and international level. He has 15 years teaching cum research experience in various institutions.

Dr. Shailendra Narayan Singh received his doctorate in CSE in 2012 and master degree from PTU, Punjab. He published more than 50 research papers in repute journals and conferences at national and international level. He has 21 years teaching cum research experience in various institutions. His research area is Wireless Sensor Networks, Data Mining and Operating System. He also worked at various repute positions in several repute organizations at present he is working with Amity University, Noida (UP), India.