International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 5 997 – 1004

An Overview on Message Authentication in Wireless Sensor Networks Based on Analysis of Block Cipher Algorithm

Sonam Bais [a], Prof. Animesh Tayal [b]

[a] *Department of computer Technology (WCC), Nagpur , India.*
[b] *Asstt. Professor, Department of Computer Technology, PCE, Nagpur, India.*

Abstract—Message authentication is one of the most efficient ways to prevent unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). That's why, numerous message authentication proposals have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. Many of them, however, have the restrictions of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks.

Wireless Sensor Networks (WSN) are being very popular day by day, however one of the main concern in WSN is its limited resources. One have to look to the resources to generate Message Authentication Code (MAC) keeping in mind the feasibility of method used for the sensor network at hand. This paper investigates different cryptographic approaches such as symmetric key cryptography and asymmetric key cryptography. Furthermore, it discusses encryption technique such as block cipher (consider RC6).

*****

I. INTRODUCTION

Message authentication [1] performs a very important role in thwarting unauthorized and corrupted messages from being delivered in networks to save the valuable sensor energy. Therefore, many authentication schemes have been proposed in literature to offer message authenticity and integrity verification for wireless sensor networks (WSNs) [5]–[9]. These approaches can largely be separated into two categories: public-key based approaches and symmetric-key based approaches.

The symmetric-key based approach necessitates composite key management, lacks of scalability, and is not flexible to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The shared key is handled by the sender to produce a message authentication code (MAC) for each transmitted message. However, for this process the authenticity and integrity of the message can only be confirmed by the node with the shared secret key, which is usually shared by a group of sensor nodes. An intruder can compromise the key by incarcerating a single sensor node. In addition, this method is not useful in multicast networks.

For the public-key based method, each message is transmitted along with the digital signature of the message produced using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key [10], [11]. One of the restrictions of the public key based method is the high computational overhead.

II. TERMINOLOGY AND PRELIMINARY

This section briefly describes the terminology and the cryptographic tools.

A. Threat Model and Assumptions

The wireless sensor networks are implicit to consist of a huge number of sensor nodes. It is assumed that each sensor node recognizes its relative location in the sensor domain and is competent of communicating with its neighboring nodes directly using geographic routing. The entire network is fully connected through multi-hop communications. It is assumed that there is a security server (SS) that is liable for generation, storage and distribution of the security parameters among the network. This server will by no means be compromised. However, after deployment, the sensor nodes may be compromised and captured by attackers. Once compromised, all data stored in the sensor nodes can be obtained by the attackers. The compromised nodes can be reprogrammed and completely managed by the attackers.

However, the compromised nodes will be unable to produce new public keys that can be accepted by the SS and other nodes. Two types of possible attacks launched by the adversaries are:

• *Passive attacks*: By passive attacks, the adversaries could snoop on messages transmitted in the network and execute traffic analysis.

• *Active attacks*: Active attacks can only be commenced from the compromised sensor nodes. Once the sensor nodes are compromised, the adversaries will gain all the data stored in the compromised nodes, including the security

parameters of the compromised nodes. The adversaries can alter the contents of the messages, and introduce their own messages.

An authentication protocol should be resistant to node compromise by allowing secure key management. The protocol may provide an integrated key-rotation mechanism or allow for key rotation by an external module.

III. LITERATURE REVIEW

In papers [5], [6], symmetric key and hash based authentication techniques were projected for WSNs. In these techniques, each symmetric authentication key is shared by a cluster of sensor nodes. An intruder can compromise the key by capturing a single sensor node. Therefore, these techniques are not flexible to node compromise attacks. A secret polynomial based message authentication technique was discussed in [7]. This scheme presents information-theoretic security with ideas akin to to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. When the number of messages transmitted is lower the threshold, the technique facilitates the intermediate node to confirm the authenticity of the message through polynomial evaluation.

However, when the number of messages transmitted is greater than the threshold, the polynomial can be fully improved and the system is completely broken. To boost the threshold and the complexity for the intruder to reconstruct the secret polynomial, a random noise, also called a perturbation factor, was introduced to the polynomial in [8] to thwart the adversary from calculating the coefficient of the polynomial. However, the added perturbation factor can be entirely removed using error-correcting code schemes [12]. For the public-key based ap technique, each message is transmitted along with the digital signature of the message produced using the sender's private key. Every intermediate forwarder and the last receiver can authenticate the message using the sender's public key. The recent development on elliptic curve cryptography (ECC) focuses that the public-key schemes can be more beneficial in terms of memory usage, message complexity, and security resilience, since public-key based techniques have a simple and clean key management [13].

Wireless sensor networks (WSN) have the lead over traditional networks in numerous ways such as large scale, autonomous nature and intense deployment [1] [14]. Likewise, it has improved fault tolerance because if a sensor node fails others can gather/proceed data. Because of its ad-hoc nature it grows to be more attractive in certain applications such as syndrome surveillance, military, environmental observation, fire detection, supply chain management, energy automation, vision enabling, gaming, building administration, health and other commercial and home applications [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28].

With the extensive deployment of WSN for multi-faceted applications security is becoming a growing concern. For example, in a battleground, a military communication network used for susceptible information exchange can be hacked by its adversaries if the WSN has security holes causing stern loss of life and machinery. Security of WSN is a big challenge due to its limited resources such as power supplies, energy, computation, small memory and communication capabilities [29], [30], [31], [32], [14].

Cryptographic algorithm performs a significant role in the security and resource conservation of wireless sensor networks (WSN) [33], [34]. This paper spotlights a cryptographic and encryption scheme that produces Message Authentication Code (MAC) in wireless sensor networks (WSN), which is more practicable in the restricted resources of wireless sensor networks (WSN) and also supply good security in communication as well.

IV. INSIDE VIEW ON WIRELESS SENSOR NETWORKS

Wireless sensor networks simplify the compilation and scrutiny of information from multiple locations [3]. The term wireless sensor network (WSN) illustrates an association among miniaturized embedded communication devices that supervise and evaluate their surrounding environment. The network is composed of many minute nodes sometimes referred to as motes [35]. A node is made up of the sensor(s), the microcontroller, the radio communication component, and a power source. Wireless sensor nodes range in size from a few millimeters to the size of a handheld computer. Apart from of size, sensor nodes share general constraints. This section recognizes the exclusive challenges of wireless sensor networks.

A. Characteristics of Wireless Sensor Networks

Wireless sensor networks are deployed for a varied diversity of applications, each characterized by a exclusive set of requirements. While the classical sensor network made up of homogeneous devices, contemporary sensor networks fit in modular design and make use of heterogeneous nodes that accomplish unique requirements. For example, some nodes contain a GPS sensor that other nodes can query to decide their location. Others may contain interfaces to the Internet through satellite or cellular communications. While radio frequency is the most general communication modality, data can also be transmitted via laser, sound, and diffuse light. These communication means carry an assortment of network infrastructures.

In a fundamental infrastructure-organized network, nodes can only converse with a base station. The reverse is true in an ad-hoc network where there is no base station or communication infrastructure. In this case, each node can converse with any other node. The communication infrastructure manipulates network topology. In some cases, each node must be inside radio range of any other node because messages can only voyage across a single hop. Networks planned into a graph-like topology permit routing of messages across multiple hops. Some applications can achieve their goals with a network of sparsely deployed sensors. Others require a densely populated network with redundant nodes accessible.

Network topology and coverage requirements decide the network size. Networks may range in size from thousands of nodes to only a few.

B. Security in WSN

Security risks in wireless sensor networks contain threats to the confidentiality, integrity, and availability of the system. Security methods used on the Internet are not simply adaptable to sensor networks because of the limited resources of the sensors and the ad-hoc feature of the networks. The adoption of competent algorithms to alleviate security risks has not kept pace with the rate of miniaturization. This section underscores the challenges of securing sensor network communications and demonstrates general attacks against sensor networks.

1. Security Goals

Security assessments of any application spotlight on the five fundamental tenets of data security: confidentiality, origin integrity, data integrity, non-repudiation, and availability. The definitions used in this subsection are derived from [36] and [37].

Confidentiality means the camouflage of information from unauthorized entities. Mechanisms used to accomplish confidentiality include access control mechanisms and cryptography. Cryptography scrambles, or encrypts, information to produce cipher text inarticulate to any unauthorized viewer. The data can be made understandable to an authorized viewer who knows the secret key. Semantic security entails a stronger assurance of confidentiality. Semantic security needs that repeated encryption of a message *M* would yield unique cipher text each round. This confines the ability of an eavesdropper to understand the plaintext even after observing numerous encryptions of the identical message. Use of initialization vectors (IVs) seeded with a counter or a non-repeating nonce gives semantic security.

Origin integrity, also recognized as authentication, refers to the trustworthiness of the source of information. It means that the receiver of a message can trust that the sender of the message is candidly who it claims. An intruder should be unable to propel a fabricated message and have it treated as a legitimate message from a trusted peer. Data integrity means that the user of the information can trust that the content of the information has not been altered in any way by an unauthorized intruder or improperly customized by an authorized user. Since alike mechanisms present origin integrity and data integrity, they are usually grouped under the moniker "integrity". Integrity outshines other security goals because of its influence on the reliability of the system and its output. In a robust wireless sensor network, the data contained in a message grips a lower priority than the integrity and authenticity of the message.

Non-repudiation means that the sender of a message should not be able to reject later that he ever sent that message. In the pre-digital scenario, one achieved non-repudiation with a simple hand-written signature. In cryptography, it implies that authentication and data integrity can be certified with a high level of guarantee and it cannot later be refuted. Non-repudiation is a serious security service and must be guaranteed in applications that engage financial and business transactions, where accountability of events is significant to guarantee success of the applications. Digital signatures offer non-repudiation.

Availability implies that an authorized user should be able to employ the data or resource as required. In a wireless sensor network, the wireless communication link must remain obtainable for the network to sustain operations.

2. Challenges

The lack of proficient authenticated messaging exposes all layers of the sensor network protocol stack to potential compromise. Without link-layer authentication, an attacker may insert unauthorized packets into the network. This may be used to introduce collisions and force legitimate nodes into an infinite waiting state [38]. Network layer attacks against routing protocols give the attacker the ability to cause routing loops, delay messages, or selectively drop messages [39]. Wireless sensor networks deployed for tracking targets provide valuable application layer notifications about the location of the target. Without authentication, the attacker can perpetrate attacks such as dropping intruder notifications, spoofing intruder notifications to create a diversion, or forcing the entire network into a continual state of reorganization.

In wireless sensor networks, the need for integrity surpasses all other security goals. Data integrity and authentication create a foundation for a highly available and trustworthy network. While many authentication schemes have been conceived for wireless sensor networks, none of them is a panacea. Algorithms for unicast message authentication, for

example, do not meet the requirements for authenticating broadcast messages. Similarly, algorithms that mimic the asymmetry of public key systems by dividing time into slots violate the real-time constraints of intrusion notification systems.

3. Attacks against Sensor Networks

Physical tampering poses a threat to sensors. If sensors are distributed in an unprotected area, an attacker could destroy the nodes or collect the sensors, analyze the electronics, and steal cryptographic keys. This complicates the process of bootstrapping newly deployed sensors with cryptographic keying material. To protect against this, sensors must be tamper-proof or they must erase all permanent and temporary storage when compromised. Secure key rotation mechanisms can also mitigate the threat of stolen cryptographic keys.

Jamming attacks against wireless radio frequencies affect the availability of the network. While it is most efficient to program sensors to communicate on one specific wireless frequency, an attacker could easily broadcast a more powerful signal on the same frequency and introduce interference into the communications channel. Spread spectrum technologies such as frequency-hopping spread spectrum alleviate the impact of jamming; however, complex channel hopping patterns reduce battery life. Nodes could also try to detect jamming and sleep until the jamming stops, resulting in a temporary, self-induced denial of service (DoS).

Link layer protocols face similarly challenging threats. Attackers can introduce collisions that force communicating nodes to retransmit frames. Following a collision, a node must back-off and wait for the channel to clear before attempting to resend. The attacker can continually introduce collisions until the victim runs out of power. While error-detecting mechanisms suffice for common transmission errors, they do not reduce the influence of maliciously generated collisions. Collisions maliciously injected near the end of a legitimate frame rapidly exhaust the resources of the legitimate node. Authentication cannot alleviate these physical and link layer attacks.

Network layer attacks take advantage of the ad-hoc organization of wireless sensor networks. Any node in the network can become a router, forwarding traffic from one node to another. By manipulating routing information, the attacker can shape the flow of traffic. The simplest attack compromises a routing node and forces it to drop messages, creating a network "black hole". The attacker can also selectively delay messages routed by the compromised node. In a wormhole attack, the adversary tunnels messages destined for one part of the network through a path under enemy control. Wormhole attacks facilitates eavesdropping, message replay, or disconnection of a segment of the network. One technique to create black holes circumvents the way routing protocols organize the network. Nodes typically accept the router that broadcasts route advertisements with the strongest radio signal. This policy reduces the energy required for a node to converse with its default router. An attacker can influence this strategy to convince legitimate nodes that it necessitates the least communication overhead.

Internet style attacks have their analogue in wireless sensor networks. Misdirection attacks, such as the Internet smurf attack, work in sensor networks. The attacker can propel multiple messages to broadcast addresses with a source address forged to the intended victim's address. The broadcast retorts will overwhelm the victim, flood its communication channel, and exhaust its power. Filtering the legitimate messages from the responses in a smurf attack needs a hierarchy not present in many wireless sensor network routing protocols.

A alike attack, called a Sybil attack, objects systems that choose peers based on their reputation. In a Sybil attack, the adversary sends a large number of fabricated messages that emerge to be forwarded from other nodes. Legitimate nodes commence to trust the attacker because it seems to fairly route traffic. The legitimate nodes will eventually accept the adversarial node as their router.

Transport-layer protocols present end-to-end connectivity between nodes. Sequencing, such as that done in the Transmission Control Protocol (TCP), enhances the reliability of the connection. Protocols that apply sequencing may yield to Denial of Service (DoS) attacks. The classic TCP SYN flood concerns to sensor networks. An adversary can flood the victim with synchronization requests and bound the ability for other nodes to converse with the victim. One solution limits the number of synchronization needs accepted, but this limits both adversaries and allies. Client riddles, a more complex solution, require the client to construct a commitment to the server before it is allowed to begin a conversation. When the client opens a connection, the server will reply with a puzzle that the client must crack. The client must solve the puzzle and propel the answer to the server before the server will recognize a full connection. While this solution defend the server from SYN floods, it may damage allies that have fewer computational resources than the adversary does.

Origin authentication and message integrity can alleviate attacks at the network layer and above. Threats such as spoofing or fabrication of routing data validate the need for origin and data integrity of even the simplest HI.

V. REVIEW OF MESSAGE AUTHENTICATION PROTOCOLS

This section summarizes some of the most relevant proposals that incorporate origin integrity and data integrity in to wireless sensor network communications. Each proposal possesses exclusive qualities that persuade its applicability. Many merge schemes for origin integrity and message integrity with other security goals, such as confidentiality or replay protection. However, these features may use excessive processor, storage, or energy resources.

An authentication protocol should be defiant to node compromise by permitting secure key management. The protocol may offer an integrated key-rotation mechanism or permit for key rotation by an external module. In addition, the protocol must have small computation overhead for both the sender and the recipient of a message. The protocol must also necessitate low communication overhead. Finally, messages supporting the authentication protocol must purpose in an unreliable network. Thus, the protocol should support the ability to immediately authenticate a message upon receipt.

Cryptographic Constructs

A. View on Conventional Authentication

The roots of message integrity commence with cryptographic checksums, also known as hashes. These checksum functions acquire a message and compact it into a smaller message digest [36]. The simplest example, the parity bit, calculates the number of 1-bits in a message to create a checksum of 1-bit in length. Strong cryptographic hash functions must own three desirable properties. First, the hash must be easy to calculate, not consuming major computational resources. Second, it should be computationally not feasible to reverse the hash function. This means that known the result of the hash $h(M)$, one should not be capable to decide M. A third advantageous property of hashing algorithms says that two distinct messages, when hashed, will acquiesce two distinct checksums. However, as per the pigeonhole principle, there is a possibility that two distinct messages M and M', will acquiesce generate the same hash value, $h(M) = h(M')$. This condition, known as a collision, can be subjugated to overcome hash functions [40]. The MD5 [41] and SHA-1 [42] hash functions are engaged in several security applications and protocols. MD5 abbreviates a message into a hash of 16 bytes. SHA-1 abbreviates a message into a 20-byte hash. Both MD5 and SHA-1 have been established susceptible to collisions [40, 43].

Hash functions give a level of message integrity between communicating peers. A sender organizes a message M and computes the checksum $x = h(M)$. It then propels the checksum along with the message to the recipient. When the recipient obtains message M, he can recompute the checksum on the received message M. If the checksum added to the message matches the checksum calculated by the recipient, then the recipient can be assured of message integrity.

Cryptographic checksums cannot give assurance that messages reach without modification or that they initiate from an authentic sender. Since an attacker may recognize the hashing algorithm in use, an attacker could just restore message M with message M', calculate the hash $x' = h(M')$, and send the concatenation of the message M' and the hash x'. The recipient will compute the hash of M', which will match the x' sent by the attacker. Thus, the recipient cannot authenticate that authenticity of the message. Message authentication codes (MAC), an instantiation of hashes that applies a unique key, give both the data integrity of checksums and origin integrity provided by a secret key. Both the sender and receiver should share the key. If an adversary finds out the secret key, the hashing function is compromised.

A MAC is generated by encrypting a message with a block cipher in Cipher Block Chaining (CBC) or Cipher Feedback Modes (CFB) [14]. Use of the Cipher Block Chaining mode to create a MAC is commonly known as CBCMAC. Several WSN authentication mechanisms utilize CBC-MAC. However, the CBCMAC operation has been shown to be apprehensive for variable length messages [44].

B. Unicast vs. Broadcast Authentication

Unicast authentication gives the assertion of origin integrity when a message is delivered from one sender to one receiver. A message authentication code (MAC), created by the sender/creator of the message by using a secret key, can be used to guarantee origin integrity. For unicast messages, static symmetric (shared) key cryptography gets the requirements because the two peers are trusted not to disclose the key. The speed and effectiveness of symmetric key cryptography suit the constraints of wireless motes.

Broadcast authentication guarantees that multiple recipients of a message can authenticate its origin integrity. If using MACs to make sure broadcast authentication, all recipients of the message must share the symmetric key. The exclusive challenge for broadcast authentication engages the management of that shared key. If the key is broadcast to probable recipients, an adversary could eavesdrop on the key broadcast, detain the key, and produce a legitimate MAC for a forged message. Public key cryptography explains the problem of securely sharing a key for conventional Internet computing systems. However, public key cryptosystems use far too a lot of storage, computation,

and bandwidth resources to be provided in wireless sensor networks.

C. *Block Ciphers*

Symmetric key cryptography have two categories of ciphers: block ciphers and stream ciphers. Stream ciphers work on a single bit or byte at a time. Block ciphers function on groups of bits called blocks [37]. Common block ciphers considered for wireless sensor networks admit block sizes of 32, 64, and 128 bits. Authentication mechanisms typically utilize block ciphers because they can be used to create MAC.

Table 1 summarizes the block and key sizes of common block ciphers.

Table 1: General Block Ciphers

Ciphers	Key Size(b)	Block Size(b)
AES	128/192/256	128
RC5	0 ~ 2040	32/64/128
RC6	128/192/256	128
Twofish	128/192/256	128
Skipjack	80	64
XTEA	128	64

Cipher Key Size (b) Block Size (b)

Symmetric key encryption is frequent to ensure data confidentiality, it utilizes shared key for both encryption of plain text and decryption of cipher text. In cryptography, the Advanced Encryption Standard (AES) [45] is an encryption standard adopted by the U.S. government.

A combination of factors such as security, performance, efficiency, easiness of implementation and flexibility contributed to the assortment of this algorithm as the AES. RC6 [46], Twofish [47] and Rijndael [48] were designed to match the requirements of the Advanced Encryption Standard (AES) competition. Following subsection focuses only on RC6 for Authentication mechanisms typically employing block ciphers to generate MAC.

VI. ANALYSIS ON RC6

RC6 is derivative from RC5 [49]. There are two main new features in RC6 compared to RC5: the enclosure of integer multiplication and the employ of four w-bit working registers instead of two w-bit registers as in RC5. It was designed by Ron Rivest, Matt Robshaw, Ray Sidney and Yiqun Lisa Yin [50].

RC6 is very alike to RC5 in structure, using data-dependent rotations [49], addition modulo 2^w and XOR operations; actually, RC6 could be considered as interweaving two parallel RC5 encryption processes. However, RC6 does utilize an extra multiplication operation not present in RC5 in order to formulate the rotation dependent on every bit in a word and not just the least significant few bits. Integer multiplication is used to enhance the diffusion achieved per round so that fewer rounds are needed and the speed of the cipher can be increased. The base-two logarithm of w will be indicated by lg w.

Similar to RC5, RC6 is a completely parameterized family of encryption algorithms. A version of RC6 is more precisely specified as RC6-w/r/b where the word size is w bits, encryption has nonnegative number of rounds r and b denoting the length of the encryption key in bytes. Since the AES submission is aimed at w = 32 and r = 20, it can use RC6 as shorthand to consider to such versions. When any other value of w or r is intended in the text, the parameter values will be specified as RC6-w/r. Of meticulous relevance to the AES attempt will be the versions of RC6 with 16-, 24- and 32-byte keys. For all variants, RC6-w/r/b works on units of four w-bit words using the following fundamental operations [51].

The operations used in RC6 are given as followings.

A+B integer addition modulo 2^w
A-B integer subtraction modulo 2^w
A⊕B bitwise exclusive-or of w-bit words
A*B integer multiplication modulo 2^w
A<<<B rotation of the w-bit word A to the left by the amount given by the least significant lg w bits of B
A>>>B rotation of the w-bit word A to the right by the amount given by the least significant lg w bits of B
$f(x) = x(2x+1) \bmod 2^w$

There are three modules in RC5: key expansion, encryption, and decryption. Key-Expansion algorithm is employed to produce the round sub keys that will be utilize in encryption and decryption algorithms. RC6 has different algorithms for encryption and decryption, in encryption it employs integer addition modulo 2^w but in decryption it employs integer subtraction modulo 2^w. RC6 is a symmetric key encryption so encryption and decryption algorithms uses shared key.

The authentication scheme should aim at achieving the following various objectives:

• *Message authentication:* The message receiver should be competent to authenticate whether a received message is sent by the node that is claimed or by a node in a exacting group. In other words, the adversaries cannot pretend to be a guiltless node and insert fake messages into the network without being captured.

• *Message integrity:* The message receiver should be clever to authenticate whether the message has been modified en-route by the adversaries. In other words, the adversaries

cannot alter the message information without being detected.

• *Hop-by-hop message authentication:* Every forwarder on the routing path should be capable to validate the authenticity and integrity of the messages upon reception.

• *Identity and location privacy:* The adversaries cannot settle on the message sender's ID and location by analyzing the message data or the local traffic.

• *Node compromise resilience:* The scheme should be resilient to node compromise attacks. I does not matter how many nodes are compromised, the remaining nodes can still be safe.

• *Efficiency:* The scheme should be proficient in terms of both computational and communication overhead.

VII. CONCLUSION

This paper discusses an overview on message authentication in wireless sensor networks. Message authentication performs a key role in thwarting unauthorized and corrupted messages from being forwarded in networks it investigates that public key is not energy efficient and is costly in terms of both computation and communication as compared to symmetric key. Sensor networks have limited resources, therefore most of the researcher considered symmetric key to create MAC in WSNs. Thus, paper observes that symmetric key techniques are more feasible for WSNs as compared to public key. Here block cipher (Mainly RC6) is considered as technique to create Message authentication code (MAC) in sensor network.

References

[1] Jian Li Yun Li Jian Ren Jie Wu, "Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, pp 1-10, 2013

[2] Sadaqat Ur Rehman, Muhammad Bilal, Basharat Ahmad, Khawaja Muhammad Yahya, Anees Ullah, Obaid Ur Rehman, "Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012, pp 96-101

[3] Raymond Sbrusch, "Authenticated Messaging In Wireless Sensor Networks Used For Surveillance", Thesis, The University Of Houston-Clear Lake, May, 2008

[4] Harsh Kumar Verma, Ravindra Kumar Singh, "Performance Analysis of RC6, Twofish and Rijndael Block Cipher Algorithms", International Journal of Computer Applications (0975 – 8887) Volume 42– No.16, March 2012, pp 1-7

[5] F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," in IEEE INFOCOM, March 2004.

[6] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks," in IEEE Symposium on Security and Privacy, 2004.

[7] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in Advances in Cryptology - Crypto'92, ser. Lecture Notes in Computer Science Volume 740, 1992, pp. 471–486.

[8] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromise resilient message authentication in sensor networks," in IEEE INFOCOM, Phoenix, AZ., April 15-17 2008.

[9] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in IEEE Symposium on Security and Privacy, May 2000.

[10] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications. of the Assoc. of Comp. Mach., vol. 21, no. 2, pp. 120–126, 1978.

[11] T. A. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.

[12] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking cryptographic schemes based on "perturbation polynomials"," Cryptology ePrint Archive, Report 2009/098, 2009, http://eprint.iacr.org/.

[13] H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control," in IEEE ICDCS, Beijing, China, 2008, pp. 11–18.

[14] Matthew N. Vella, Texas A&M University-Corpus Christi, Computer Science Program, Dr. Ahmed Mahdy Texas A&M University-Corpus Christi, Computer Science Faculty "Survey of Wireless Sensor Network Security"

[15] Chung-Kuo Chang, J. Marc Overhage, Jeffrey Huang "An Application of Sensor Networks for Syndromic Surveillance" 2005 IEEE

[16] Dunfan Ye,DaoliGong,WeiWang "Application of Wireless Sensor Networks in Environmental Monitoring", 2009 2nd International Conference on Power Electronics and Intelligent Transportation System.

[17] Ling Tan, Shunyi Zhang, and Yanfeng Sun, Jing Qi "Application of Wireless Sensor Networks in Energy Automation", Sustainable Power Generation and Supply, 2009. Supergen '09. International conference

[18] Sundip Misra, Vivek Tiwari and Mohammad S. Obaidat, Fellow, IEEE "LACAS: Learning Automata-Based Congestion Avoidance Scheme for Healthcare Wireless Sensor Networks", IEEE Journal on Selected Areas in Communications, Vol. 27, No. 4, May 2009

[19] Ian F. Akylidiz, Fellow IEEE, Tommaso Melodia, Member IEEE, and Kaushik R. Chowdhury, Student Member IEEE "Wireless Multimedia Sensor Networks: Applications and Testbeds", Proceedings of the IEEE. Vol. 96, No. 10, October 2008

[20] Kwangsoo Kim, Jongarm Jun, Sunjoong Kim, and Byung Y. Sung "Medical Asset Tracking Application in Wireless Sensor Networks", The Second International Conference on Sensor Technologies and Applications, 2008 IEEE

[21] N. Rajendran, P. Kamal, D. Nayak, and S. A. Rabara, " WATSSN: A Wireless Asset Tracking System using Sensor Networks", Proceedings of IEEE International Conference On Personal Wireless Communications, Jan 2005

[22] G. W. Allen, K. Lorinca, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, and J. Lees, "Deploying a Wireless Sensor Network on an Active Volcano", IEEE Internet Computing, IEEE Computer society, March/April 2006

[23] K. Chintalapudi, T. Fu, J. Paek, N. Kothari, S. Rangwala, J.Caffrey, R. Govindan, E. Johnson, "Monitoring Civil Structures with a Wireless Sensor Network", IEEE Internet Computing, IEEE Computer society, March/April 2006

[24] I. Ituen and G. Sohn, "The Environmental Applications of Wireless Sensor Networks", International Journal of Contents, Vol.3, No. 4, Dec 2007

[25] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, J. Anderson, "Wireless Sensor Networks for Habitat Monitoring", WSNA'02, Sep 2002

[26] Anthony Rowe, Dhiraj Goel, Raj Rajkumar "FireFly Mosaic: A Vision-Enabled Wireless Sensor Networking System", 28th IEEE International Real-Time Systems Symposium. 2007 IEEE

[27] E. Sazonov, K. Janoyan, and R. Jha, "Wireless Intelligent Sensor Network for Autonomous Structural Health Monitoring", Proceedings of Structural Materials Technology (SMT): NDE/NDT for Highways and Bridges, 2004

[28] http://corporate.traffic.com

[29] Xiaojiang Du, North Dakota State University and Hsiao-Hwa Chen, National Cheng Kung University "Security in Wireless Sensor Networks" IEEE Wireless Communication August 2008

[30] Sung-Chul Jung , Hyoung-Kee Choi. School of Information and Communication Engineering "An Energy-aware Routing Protocol Considering Link-Layer Security in Wireless Sensor Networks." Feb.15-18, 2009 ICACT 2009

[31] Md. Anisur Rahman and Mitu Kumar Debnath "An Energy-Efficient Data Security System for Wireless Sensor Network" Proceedings of 11th International Conference on Computer and Information Technology (ICCIT 2008) 25-27 December, 2008, Khulna, Bangladesh

[32] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong "Security in Wireless Sensor Networks: Issues and Challenges" Feb. 20-22, 2006 ICACT 2006

[33] Mohammad AL-Rousan, A.Rjoub and Ahmad Baset "A lowenergy security algorithm for exchanging information in wireless sensor networks", Journal of information assurance and security 4 (2009) 48-59.

[34] Y.W. Law, S. Dulman, S. Etalle, P. Havinga (2002), "Assessing security critical energy efficient sensor network", Available at: http://www.dsv.su.se/~matei/bin/4%20-%202i1279/L5_EYES.pdf

[35] Pister, K., "29 Palms fixed/mobile experiment: Tracking vehicles with a UAV delivered sensor network," 2001.

[36] Bishop, M., Computer security: art and science. Boston, MA: Addison-Wesley, 2003.

[37] Schneier, B., Applied cryptography : protocols, algorithms, and source code in C, 2nd ed. New York: Wiley, 1996.

[38] Wood, A. D. and Stankovic, J. A., "Denial of service in sensor networks," IEEE Computer, vol. 35, pp. 54-62, 2002.

[39] Wood, A. D., Fang, L., Stankovic, J. A., and He, T., "SIGF: a family of configurable, secure routing protocols for wireless sensor networks," Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, pp. 35-48, 2006.

[40] Wang, X. and Yu, H., "How to Break MD5 and Other Hash Functions," Advances in Cryptology – EUROCRYPT 2005, pp. 19-35, 2005.

[41] Rivest, R., "The MD5 Message-Digest Algorithm, RFC 1321," IETF, 1992.

[42] Eastlake, D. and Jones, P., "US Secure Hash Algorithm 1 (SHA1), RFC 3174," IETF, 2001.

[43] Wang, X., Yin, Y. L., and Yu, H., "Collision search attacks on SHA1," Crypto 2004, August 15-19, 2004.

[44] Bellare, M., Kilian, J., and Rogaway, P., "The security of the cipher block chaining message authentication code," Journal of Computer and System Sciences, vol. 61, pp. 362-399, 2000.

[45] "Report on the Development of the Advanced Encryption Standard (AES).", "csrc.net". Available at: http://csrc.nist.gov/encryption/aes/round2/r2report.pdf

[46] Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L.Yin, The RC6 TM Block Cipher, M.I.T. Laboratory for Computer Science, 545 Technology Square, Cambridge, MA 02139, Version 1.1 - August 20, 1998. Available at: http://people.csail.mit.edu/rivest/Rc6.pdf

[47] Bruce Schneier, John Kelsey, Doug Whiting ,David Wagner, Chris Hall, Niels Ferguson, "Twofish: A 128-Bit Block Cipher", 1998, [online] Available at: http://www.certainkey.com/resources/article/twofish.pdf

[48] W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice-Hall, New Jersey, 1999.

[49] "RC6® Block Cipher", "rsa.com". Available at: http://www.rsa.com/rsalabs/node.asp?id=2512

[50] "RC6", "wikipedia.org". Available at: http://en.wikipedia.org/wiki/RC6

[51] Abdul Hamid M. Ragab, Nabil A. Ismail, Senior Member IEEE, and Osama S. Farag Allah, "Enhancements and Implementation of RC6TM Block Cipher for Data Security", IEEE Catalogue No. 01 CH37239-0-7803-7101-1/01 © 2001 IEEE.