ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Security Protocol for Wi Sense based Wireless Sensor Networks

Aronee Dasgupta[1], Pritam Gajkumar Shah[2]
[1]Department of Telecommunications, RV College of Engineering, Bangalore, India.
[2]Department of Computer Science and Engineering, RV College of Engineering, Bangalore, India.

ABSTRACT: Wireless Sensor Networks have emerged as one of the leading technologies. These networks are to monitor crucial environmental parameters of humidity, temperature, wind speed, soil moisture content, UV index, sound, etc. and then transfer the required information to the base station. However, security remains the key challenge of such networks as critical data is being transferred especially when sensor nodes are used in military application in hostile territories. Most sensor nodes currently deployed have constraints on memory and processing power and hence operate without an efficient security protocol. Hereby we propose a protocol which is lightweight and is secure for wireless sensor applications. The protocol is robust and has been tested on a sensor network made up WiSense nodes.

KEYWORDS: Wireless sensor nodes; WiSense; Encryption; Decryption; AES; protocol optimizations.

I.INTRODUCTION

Due to developments in analogue and digital technologies many corporations have developed low power and low cost wireless sensor nodes which are used to provide sensing of environmental parameters [1]. Sensor nodes process the information gathered and then transmit the only the required data either to the coordinator or to the other slave nodes to provide an intelligence for better understanding of the environment (depending upon the network topology) [2] . Applications include perimeter monitoring, vehicle emission monitoring, defense monitoring (in reconnaissance scenarios), etc. Openness of the channel and low physical protection of the channel poses a security risk.

The current encryption standards had been designed for high performance devices and are taxing on the sensors which have low computation capabilities and have low available bandwidth which are used in the sensor networks. Even so, security protocols developed for ad hoc networks cannot be applied directly for sensor networks due to difference in their architecture design. Sensor networks are self-organizing, dynamic, with peer to peer data transmission capabilities sensor networks on the other hand have a well-defined topology with a central base station to which all the data is relayed. Employing traditional encryption algorithms in the sensor would cause extra bits to be processed and transmitted and due to the large processing delay incurred jitter and lag would occur throughout the network [3] . There is a paramount need for developing a robust encryption which does not heavy cryptography processes but still provides the sufficient security for the required application.

Implementing a robust yet lightweight algorithm is needed not just in the central base station but also the sensor nodes. There was a controversy regarding the implementation of AES algorithm for encryption and decryption in sensor networks utilizing the ZigBee protocol because AES needs high processing power and memory usage especially in nodes containing low amounts of available RAM [4]. Also the management and modification of the encryption keys in the sensor nodes is major consideration as the nodes are spatially distributed and thus remains away from direct human interaction for a long time. The proposed protocol uses a combination of substitution using a S-Box matrix and an XOR operation with a key to provide a reasonable level of security for low performance nodes.

II. LITERATURE REVIEW

Figure1 [5] shows a typical wireless sensor network architecture consisting of various sensor nodes connected to the sink node. The sink can be controlled by a remote terminal over the Internet. Sensor networks comprise many nodes spatially distributed over a large area. Sensor nodes are designed to work for long durations of time (possibly stretching into months) to collect, analyze and return data to base station [5].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

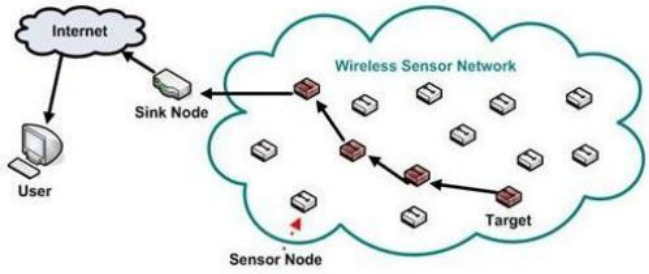

Figure 1: Wireless Sensor Network Architecture.

The sensor network may have the nodes designed as passive or active. In a passive node the base station listens to the node (and the node transmits the data back to the base station) only for a fixed duration in a time interval. This reduces the battery consumption of the node as the node can run in idle or low-power mode when the base station is not listening. A duty cycle is defined for the passive node sensor network. Duty cycle is the ratio between the active state and the low power state of the node. A smaller duty cycle helps in achieving better energy efficiency in the sensor network which is desirable [6]. In an active node the base station continuously listens to the node and the node processes, analyzes and returns the data gathered back to the base station.

In mobile sensor network each node needs to know each its location either through GPS or any other relative positioning algorithm. For ad-hoc fixed networks network information has to dynamically updated in real time as sensor nodes may fail or be added to the network. The transmission protocols and software design have to be constructed keeping in mind the effects of shallow fading, number of links, communication length, mode of propagation and the minimum acceptable quality of service. Since the sensor nodes are highly susceptible to environmental parameters (like wind speed, humidity, rain, etc.) redundancy in the number of nodes have to be provided so that the network doesn't go offline.

Security protocols have to be built into the initial design of the nodes and not as a retrofit as most nodes operate in hostile conditions and it is imperative their presence remains undetected. They are limited in their available energy (around 20 – 30 joules). Since data is arriving from large number of sources the incoming data needs to be combined with the local information so that the resulting information can be passed on to the central node. Dissemination of the large amounts of data collected and processed needs the network to have to low amounts of transmission latency. Security protocols have to be designed which protects the network from spoofing and intrusion.

2.1.WiSense Node Architecture

Figure 2: WiSense Node –courtesy WiSense [7].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Figure2 shows the WiSense WSN1101L [7] based wireless mesh node. It consists of the microcontroller module (MSP430G2955) and the radio module (CC1101). The radio module has an antenna for receiving and transmitting the data. The MSP430G2955 is an ultra-low power microcontroller from TI with 56 KB of flash memory and 4 KB static ram memory. The standby current can reach as low as 1 micro ampere. Operating voltage of the microcontroller lies between 1.8 V – 3.6 V. The module has an on-chip 10-bit ADC channels. Peripheral support is provided on the module in the form of UAR, I2C and SPI. There is a SPI and GPIO interface to the radio module and UART or I2C or SPI or GPIO interface to sensors. An on board 32 KHz crystal provides the clock.

The radio module (CC11011) operates below the 1 GHz frequency. It is a low cost transceiver suitable for remote sensing applications. The frequency range in which it operates lies in the 300-348 MHz, 387-464 MHz and 779-928 MHz bands [8] . On-off keying (OOK) and flexible (Amplitude-shift keying) ASK shaping are the two modulation schemes supported for RF transmission and receiving. Data rates range from 0.6 to 600 kbps. The on board antenna is an omni directional whip antenna, having a length of 117 mm. An on-board high accuracy 26 MHz crystal provides the clock for the circuit.

2.2. Issues in Implementing AES in Sensor Nodes

Symmetric techniques have the problem of key agreement, issues regarding the scalability of keys and do not provide nonrepudiation [9]. AES is considered slow and requires a lot of memory for the storing the lookup tables. AES has higher mean values for energy-latency product; the energy per bit for encryption process is around 151nJ/bit for 128 bit AES encryption. [10] . Even if the AES encryption takes only 11 cycles the full program with data retrieval, encryption and calculation takes a full 704 clock according to Hodjat. The decryption process was found to take 20-30% more energy than the decryption process. Also symmetric techniques like AES, are highly architecture dependent [11] .

2.3. Limitations in implementing AES in Wi Sense Nodes

The WiSense [7] node under consideration, is built on the TI MSP430G2955 a 16-bit RISC architecture based microcontroller [12]. There exist serious limitations in implementing symmetric encryption algorithms in 16-bit microcontrollers like the MSP430. Most of these algorithms are adapted for 32-bit processors; however the node under consideration is a 16-bit microcontroller. Rijndael cipher block have been optimized for 32-bit processors but these optimizations cannot be applied to the TI MSP430 due to its limited instruction set. Also these optimizations even if applied will take majority of the memory available from the node. The MSP430 has a simple but limited instruction set. The majority of register operations take up 1 cycle, but accessing the actual memory is costly and takes up to 3 cycles. Considering an example if we were to use the standard 128 bit implementation of AES in TelosB note [13], it would take 1.994 ms for encryption and a further 2.365 ms for decryption [14].

III.NETWORK ARCHITECTURE

3.1. Wi-Sense Network

We have taken into consideration a multihop mesh WiSense Sensor-Actuator Network (WISAN) consisting of 25 nodes with total of 72 sensors operating at 2405Mhz with a transmission power of 5 dbm. The sensor nodes collect data regarding temperature, voltage and pressure. The coordinator node has a MAC ID of 0xDEADBEEFFEEDDADD [15]. Table 1 shows the sensor information concerning the last and final update time tags. Table 2 shows the location and address of the nodes as they are spatially distributed in the environment. The node is based on the TI MSP430G2955 microcontroller. The module consists of two PCB's. One PCB hosts the microcontroller while the other hosts the CC1101 radio. The microcontroller PCB has 56 KB of flash, 4 KB of SRAM with a standby current (in LMP3) as low as 1 micro amp. It has as an optional on board serial to USB interfaced (to provide both power and serial connectivity). It has peripheral support in the form of SPI/I2C/UART with a 32 kHz crystal as a real-time clock [7].

Table1: Sensor Information

Name	*Id*	*Last Update*	*Next Update*
0002	1	2015-10-18 04:04:57	-
0013	1	2015-10-18 02:03:13	2015-10-18 04:03:13
0019	4	2015-10-18 01:38:33	2015-10-18 04:38:33
0014	1	2015-10-18 01:16:00	2015-10-18 04:16:00
0005	3	2015-10-17 23:49:14	2015-10-18 00:49:14
0004	2	2015-10-17 22:38:40	2015-10-18 00:38:40

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

000F	2	2015-10-17 18:03:57	2015-10-17 18:08:57
0013	5	2015-10-17 17:03:04	2015-10-17 20:03:04
0006	2	2015-10-17 16:32:14	2015-10-17 17:32:14
0010	3	2015-10-17 15:48:41	2015-10-17 15:49:11
0010	2	2015-10-17 15:48:40	2015-10-17 15:50:40
0010	1	2015-10-17 15:48:40	2015-10-17 17:48:40
0004	3	2015-10-17 15:48:10	2015-10-17 16:48:10
0008	3	2015-10-17 15:48:04	2015-10-17 17:48:04
0018	2	2015-10-17 15:11:41	2015-10-17 18:11:41
0002	2	2015-10-17 12:50:35	-
0004	1	2015-10-17 12:43:50	-
0008	1	2015-10-17 09:25:46	-
000D	4	2015-10-17 09:04:03	2015-10-17 12:04:03
0017	4	2015-10-17 08:59:58	2015-10-17 09:59:58
0017	3	2015-10-17 08:59:58	2015-10-17 09:04:58
0017	1	2015-10-17 08:59:57	2015-10-17 10:59:57
0008	2	2015-10-17 08:53:28	-
0011	3	2015-10-17 07:30:49	2015-10-17 10:30:49
000D	2	2015-10-17 07:30:45	-
0006	4	2015-10-17 06:42:23	-
0012	1	2015-10-17 05:48:30	2015-10-17 05:49:00
0011	4	2015-10-17 04:38:00	2015-10-17 04:39:00
006	3	2015-10-17 03:07:38	-
000C	3	2015-10-17 02:02:56	-
0009	1	2015-10-17 01:10:27	-
000F	6	2015-10-17 00:32:06	-
0005	2	2015-10-16 23:47:16	2015-10-16 23:48:16
0014	4	2015-10-16 23:46:03	2015-10-16 23:48:03
0019	3	2015-10-16 23:34:20	2015-10-16 23:34:50
0019	1	2015-10-16 23:34:19	2015-10-16 23:34:49
000F	5	2015-10-16 23:30:06	2015-10-16 23:32:06
000F	1	2015-10-16 23:30:04	2015-10-16 23:32:04
0014	3	2015-10-16 21:05:30	2015-10-16 21:10:30
0007	1	2015-10-16 18:47:45	2015-10-16 19:47:45
0007	4	2015-10-16 18:47:45	2015-10-16 19:47:45
0014	5	2015-10-16 17:26:13	2015-10-16 17:26:43
0016	1	2015-10-16 17:21:28	2015-10-16 17:23:28
000C	4	2015-10-16 17:12:18	2015-10-16 17:12:48
000C	2	2015-10-16 17:12:17	2015-10-16 17:17:17
0007	3	2015-10-16 16:17:19	-
0011	2	2015-10-16 15:40:15	2015-10-16 15:42:15
0018	4	2015-10-16 14:21:24	-
0007	2	2015-10-16 12:36:25	-
000D	1	2015-10-16 12:33:41	2015-10-16 13:33:41
000E	3	2015-10-16 11:40:07	2015-10-16 13:40:07
000D	3	2015-10-16 09:55:55	-
000C	1	2015-10-16 09:28:08	-
0003	1	2015-10-16 09:19:50	2015-10-16 10:19:50
0006	1	2015-10-16 08:34:04	-
0017	2	2015-10-16 07:57:38	-
000F	4	2015-10-16 07:56:27	-
0018	3	2015-10-16 07:52:37	2015-10-16 07:54:37
0018	1	2015-10-16 07:52:36	2015-10-16 07:53:36
000E	2	2015-10-16 06:23:18	2015-10-16 06:28:18
0019	2	2015-10-16 05:01:43	-
0013	3	2015-10-16 04:21:11	-
0013	2	2015-10-16 03:28:17	-
0013	4	2015-10-16 03:10:35	2015-10-16 03:11:35
0014	2	2015-10-16 03:04:01	2015-10-16 03:09:01
000F	3	2015-10-16 01:42:43	-

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

0011	1	2015-10-16 01:20:02	-
000E	4	2015-10-15 23:58:14	2015-10-16 00:03:14
000E	1	2015-10-15 22:50:11	-
0011	5	2015-10-15 19:15:10	2015-10-15 19:16:10
0005	1	2015-10-15 17:46:07	2015-10-15 18:46:07
0005	4	2015-10-15 13:00:01	2015-10-15 5:00:01

-courtesy WiSense [21]

Table 2: Node Information

Name	*Location*	*MAC Address*	*Short Address*
0002	Blk-B	0x0002000200020002	0x0002
0003	North Wing	0x0003000300030003	0x0003
0004	Corridor-B	0x0004000400040004	0x0004
0005	B-A	0x0005000500050005	0x0005
0006	South Wing	0x0006000600060006	0x0006
0007	Blk-A	0x0007000700070007	0x0007
0008	Car Park	0x0008000800080008	0x0008
0009	Nw Lab	0x0009000900090009	0x0009
000A	Corridor-A	0x000A000A000A000A	0x000A
000B	South Wing	0x000B000B000B000B	0x000B
000C	South Wing	0x000C000C000C000C	0x000C
000D	Blk-B	0x000D000D000D000D	0x000D
000E	South Wing	0x000E000E000E000E	0x000E
000F	Blk-B	0x000F000F000F000F	0x000F
0010	North Wing	0x0010001000100010	0x0010
0011	North Wing	0x0011001100110011	0x0011
0012	Corridor-B	0x0012001200120012	0x0012
0013	Blk-A	0x0013001300130013	0x0013
0014	Nw Lab	0x0014001400140014	0x0014
0015	Nw Lab	0x0015001500150015	0x0015
0016	Corridor-A	0x0016001600160016	0x0016
0017	ECE Dept	0x0017001700170017	0x0017
0018	Nw Lab	0x0018001800180018	0x0018
0019	Corridor-B	0x0019001900190019	0x0019

3.2. Firmware Elements

The firmware elements consist of the Reduced Function Device (RFD), Full Function Device (FFD), Coordinator and the Gateway [16] . Reduced Function Device (RFD) is essentially a mote that has sensors and firmware code for remote connectivity and local processing. The available sensor information is relayed to the FFD from the RFD. Full Function Device (FFD) is similar to a RFD, but it also helps as an intermediate relay node. A RFD sends information to a neighboring FFD, which deals with routing that information to its neighbouring FFDs. This chain proceeds until the coordinator is reached. The PAN coordinator is the master device and the control point in the system. Various systems can exist in the same area, however, there will be one and only coordinator for every system. RFDs and FFDs partner with the coordinator when they join that specific system. The coordinator allocates every hub a PAN address that is

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

legitimate inside the system. Messages from reduced and full function devices are sent to the gateway. Control messages are prepared by the coordinator however sensor information is generally sent to gateway the for transmission

towards LAN/WAN. Explicit control messages are given to the gateway, which are then transmitted to the nodes with the coordinator acting as relay.

IV. IMPLEMENTATION

In this paper, it proposes efficient communication between CR in the Advanced Encryption Standard (AES) with Cipher Block Chains, the outcome of encryption of the first block is used to encrypt the next. The process is continued iteratively. Such a design calls for a feedback. Each round of encryption uses the following processes viz. SubBytes, Shift Rows, Mix Columns and Add RoundKey [17]. There are in total ten rounds with the last round skipping the Mix Columns step. At the receiver end a mathematical inverse of each step is done, however, the order is reversed. We consider the block size of128 bits. Other than the SubBytes step all the other three steps are linear. In the only nonlinear step (SubBytes) the Galois inverse is calculated of an 8-bit number which itself lies in the Galois Field GF (28). Despite being faster the look up table method suffers from one critical disadvantage: it occupies 256 bytes of storage not considering the memory needed for addressing and storing the results. [18] . Each 16 bytes in the block needs to processed separately and in parallel for the substation. However, for practical applications this would cause to 16 copies of the S-Box to be present for a single round itself and for a full pipeline implementation, 160 copies of the S-Box table for the entire encryption process [17]. A total of 40960 bytes of memory would be needed for the SubBytes step alone, which is expensive in sensor nodes.

4.1. Proposed Protocol

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 3: AES S-Box [19].

Figure3 [19] shows an AES S-Box. Every sensor node in the network will have an inbuilt 16*16 S-Box [20] which would occupy a total of 2 kilobits of flash memory. Now consider two nodes that wish to communicate with each other for sending and receiving humidity, temperature, wind speed, soil moisture content, UV index or sound values etc., this value to be sent is first substituted with the corresponding element in the 16*16 S-Box by the method of substitution. The substituted value is then EX-ORed with a key, which can be - a) hour/minute/second value in the timestamp b) the node name c) last two bits of its MAC address. At the receiver end the received data is again first EX-ORed with the key then mapping is done with the help of the S-Box to arrive at the unencrypted value. We consider only 2 digits of the MAC address, timestamp, or the node name as the key to save on memory. If we were to use the timestamp as the key then an extra flag should be transmitted specifying whether the hours, mins or seconds is considered as the time stamp value. The above proposed security protocol consumes the least memory of little more 2 Kilobits (along with some memory needed for the runtime code) which is important for a light weight sensor network like Wi-Sense where it is difficult to incorporate more complex security algorithms. The protocol is verified for its robustness and forms a better security protocol for wireless sensor networks.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

4.2. Example

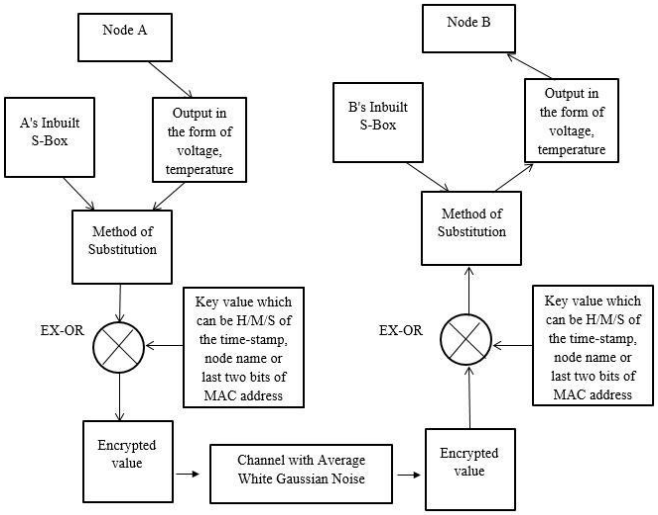

Figure 4: High level Block Diagram of the prosposed encryption and decryption process.

Figure4 shows the high-level implementation of the proposed encryption and decryption process with a block diagram. We can use the time-stamp, node name, or the MAC address as the key for the Ex-OR operation. However, we consider the MAC address as the key. If we were to take the time-stamp as the key then, we need an additional flag of 2-bit length to specify whether we are using the hours, minutes or seconds as the time-stamp value. This not only creates an extra overhead, but is also susceptible to noise in the channel. Any interference in the channel may cause bit flipping and will cause the wrong time stamp to be used at the receiver for the Ex-OR operation in the decryption process.
We consider the 8-bit data 0xD5 to be transmitted from the node 08 with a MAC address of 0x0008000800080008 (from Table 2) with the corresponding encryption and decryption process. The data first undergoes the substitution process with the S-Box, so the substituted value after the Sub Bytes operation is 03 in hexadecimal notation. The substituted value is then EX-ORed with the last two digits of the MAC address of that node (which is 0x08). The resulting encrypted value to be transmitted is 0x0B which is 8 bit in size. The data undergo packetization. The packet also contains the physical address of the source node which is the combination of IP address and the MAC address of the sending node. At the receiver node deframing is done and the 8-bit encrypted data is EX-ORed with the last digits with the MAC address. In this case, the result is 0x03. This result is now mapped to the inverse S-Box table to arrive at the decrypted value of 0xD5.

V. CONCLUSION

With the widespread adoption of wireless sensor networks to monitor and gauge environmental parameters it has become necessary to come up with a simple yet robust security protocol for hardware onstraint sensor nodes. The protocol developed was tested on the MSP430 based WiSense nodes and was found to be satisfactory in terms of performance and security. The combination of Sub Bytes and EX-OR provides a strong security against intrusion by unauthorized sources. However, further optimizations can be done to provide an optimal, secure communication infrastrcutre for wireless sensor platforms.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

VI. ACKNOWLEDGMENT

We are grateful to R.V College of Engineering Bangalore, India for helping with necessary infrastructure for carrying out the implementation.

REFERENCES

1. IF Akyildiz, W Su, et al. Wireless sensor networks: a survey, Computer Networks 2002; 38: 393-422.
2. T Raghavendra, Wireless Sensor Networks, 2004.
3. H Al-Sakib Khan Pathan, Security in Wireless Sensor Networks: Issues and Challenges, 2006.
4. SB Shammi Didla, Optimizing AES for Embedded Devices and Wireless Sensor Networks.
5. VS Rajkumar, Wireless Sensor Networks Issues and Applications, International Journal of Computer Technology and Applications, 2012; 3: 1667-1673.
6. P Archana Bharathidasan, Sensor Networks: An Overview.
7. WiSense, WiSense WSN1101L Datasheet, 2015.
8. Texas Intruments, ti.com, Texas Instruments, 2015.
9. Toivonen, Use of Symmetric And Asymmetric Cryptography in False Report, in Seminar on Network Security, 2007.
10. Potlapally, Analyzing the Energy Consumption of Security Protocols, International Symposium on Low Power Electronics and Design, 2003; 25-27.
11. Y Wang, A Survey of security issues in wireless sensor networks, IEEE Communications Surveys & Tutorial, 2006; 8.
12. Texas Instruments, TI, 2013.
13. Crossbow, "TelosB datasheet,"
14. M. T. J. P. K. M. D. S. Pierangela Samarati, "Information Security Theory and Practices: Security and Privacy of Pervasive Systems and Smart Devices," in 4th IFIP WG 11.2 International Workshop, WISTP, Passau, Germany, 2010.
15. WiSense, http://www.wisense.in/wsngui/, 2013. [Online].
16. WiSense, WiSense Documenation," WiSense, 2014.
17. V Dai Yamamoto, Performance and Security Evaluation of AES S-Box-based Glitch PUFs on FPGAs, in International Conference on Security, Privacy and Applied Cryptography Engineering, 2012.
18. E Trichina, Combinational Logic Design For Aes Subbyte Transformation On Masked Data, in International Association for Cryptologic Research, 2003.
19. W Stallings, Cryptography And Network Security Principles And Practice, Prentice Hall, 2011.
20. Selent, Advanced Encryption Standard," InSight: Rivier Academic Journal, 2010; 6.
21. WiSense, WiSense, 2013. [Online]. Available: http://www.wisense.in/wsngui/nodes.
22. WiSense, WiSense, 2013. [Online]. Available: http://www.wisense.in/wsngui/sensors.