A Novel Approach for Providing Security in SNMP Managed Sensor Networks Using Skipjack Algorithm

Geethu Krishna Kartha, Divya James

Abstract— Network Management is one of the important functionality in network Engineering. This paper proposes a methodology for security in SNMP managed sensor networks. Here we use SKIPJACK encryption algorithm for providing security in the network. IEEE1451.4 TEDS is also incorporated to provide plug and play of sensor networks. SNMP is compactable with many kind of devices used in networking, so it provides a wide variety of devices to communicate in a network independent of the manufacturers

Index Terms— Skipjack encryption algorithm, sensor networks, Simple Network Management Protocol, Management Information Base, TEDS,Smart sensornode , IEEE 1415.

◆

1 INTRODUCTION

Networks and processing systems are of growing impor tance and indeed, have become critical in business world.

The management of sensor network requires many functions like configuration of sensors, security, administration etc. Simple network management protocol is an application layer protocol used for managing the network devices [2]. SNMP is a network management protocol that has become the standard for the exchange of information in a network. Before the evolution of SNMP and other network management software, the administrator has to be physically attached to the network devices in order to access the configurations and troubleshooting data, which is a tedious task. SNMP uses one or more administrative computers called managers for managing and monitoring a group of devices called managed system. Software executing in each devices is called an agent. It acts as an interface between manager and managed system [2]. The manager sends messages to the agent to get or set a particular object of an element. The managed devices collect and store information and make this information available to the manager system using SNMP. An agent having management information translates into SNMP compactable form [2]. The SNMP architecture helps to achieve the following goals [5]:

1) Making the management functions more simpler

2) Management and operations are comparatively more flexible

3) Managing complex networks and device compatibility with the network

The SNMP provides various functions to manage the devices connected with the network using SNMP ping. Various other functions are GetRequest, GetNextRequest,GetBulkRequest, SetRequest,Trap, Response, InformRequest. The manager can get information regarding a particular device by using get commands [5]. Using SetRequest the manager can change the value of a variable. Response is send by the agent to the manager as response of any of the request messages. Trap is used by the agent to notify about alerts or special events that are to be monitored. InformRequest message is send by a manager to other manager as asynchronous notifications. To access the information each device will be having a unique identifier and SNMP uses dotted decimal notation called Object Identifier (OID) [2].

1.1CMIP (Common Management Information Protocol)

CMIP was created in 1998 by Internet Activities Board (IAB).It is more secure and powerful than SNMP, but SNMP is having very less overhead .SNMP defines only “set” actions to alter the state of managed devices while CMIP allows the definition of any kind of actions. The main feature that makes SNMP different is that it is widely available and interoperable among a variety of network components.

2 MANAGEMENT OF NETWORKS

2.1 Management Information Base (MIB)

MIB is defined for SNMP. It is a virtual database that helps SNMP to manage, control and monitor the devices in the network. Each SNMP variables in MIB are termed as objects.MIB defines objects through framework called structure of management information (SMI) [6].The SMI is similar to the schema of a Database system. It defines object name, data type, operations that can be performed on it. To increase the scalability, all managed objects are arranged in a tree structure. The leaf nodes of the tree are the actual managed objects each of which represents some activity, resource, or related information. The MIB should be compiled after its generation in

- *Geethu Krishna Kartha is currently pursuing masters degree program in networkr engineering inMahatma Gandhi University,Kottayam,Kerala,India PH-+919037114194. E-mail: geethukk1991@gmail.com*
- *Divya James is currently Working as assistant professor in IT Department ,Mahatma Gandi University,Kerala,India PH-+919037677328. E-mail: Divyajames @gmail.com*

order to make the SNMP work properly [5]. The objects in MIB are defined using Abstract syntax notation 1. Here hierarchical name space containing OIDs are used [7]. The path from the top of the tree down to the point of interest forms the OID. MIB's are updated to add new functionalities, to remove unwanted information and to fix defects [7].

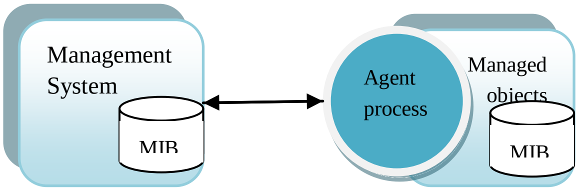


Fig1: SNMP Architecture

2.2 Skipjack: Encryption Method

Skipjack is an encryption method used in wireless sensor networks. Eli Biham and Adi Shamir discovered an attack against 16 of the 32 rounds within one day of declassification, and Alex Biryukov extended this to 31 of the 32 rounds within months using impossible differential cryptanalysis. It is easy to see an exhaustive key search as a promising attack against Skipjack due to its relatively short key length of 80-bits Skipjack uses an 80-bit key to encrypt and decrypt 64-bit data blocks. It is a 32 rounds unbalanced Feistel network [16].

2.3IEEE 1451

The sensors must have networking capabilities that supports the data flow, interoperability, compatibility and security. IEEE 1451 is a new standard of managing sensor networks [10] .It develops a vendor independent and network independent transducer interfaces. It provides many functions to make sensor smart such as:

- Self-diagnostic and self-identification
- Conforming to standard data and control protocol
- Provides Standard digital data as output
- Software functions like signal processing etc

The IEEE1451 standards are:

a. IEEE1451.1, developed in 1999 is Network Capable Application Model (NCAP) for smart transducer. It provides a Common Object model that can be used with multiple networking protocols. Uniform models for key functions needed in smart transducers including physical parametric data, application functionality and communication. It develops a framework that helps to create smart transducers.

b. IEEE1451.2 is introduced in 1997 and is known as Extensible Transducer Electronic Data Sheet (TEDS).It is basically a general calibration model for transducers. Triggering and control models define how the channel is accessed. It has power concepts of correction engine and flexible location of correction engine and contains different kinds of sensors.

c. IEEE1451.3 is Digital Communication and Transducer Electronic Data Sheet (TEDS) Formats for Distributed Multidrop Systems.

d. IEEE1451.4 Transducer Electronic Data Sheet [11].

2.4TEDS (Transducer Electronic Data Sheet)

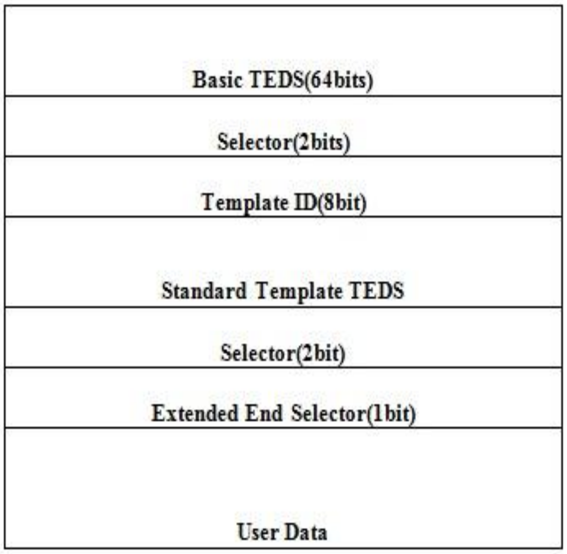


Fig 2 : Traducer with standard TEDS content

TEDS is a volatile memory inside sensor to store information. The sensor manufacturer uses this memory to store details regarding the manufacturer name, model number, serial number, sensor type and calibration data [11]. The sensor works in two different modes such as analog and digital. In the digital mode the sensor data inside the memory can be downloaded and in the analog mode the sensor basically does the functions in this mode [10] .TEDS basically is meant for plug and play of sensors. The memory in the TEDS are of two types, Volatile memory(RAM) and Permanent memory (ROM).The permanent memory stores data about the sensor manufacturer and other specification of the sensor .Volatile memory stores only the current measurement values . The IEEE 1451.4 defines TEDS as different sections chained together to form a complete TEDS. The first section is the Basic TEDS which defines the essential details regarding the sensor. Optionally, this standard template TEDS is followed by a calibration template. Two-bit selectors in the TEDS data indicate the next section of the TEDS. The end section of the TEDS is specified as open user area [11].

There are many advantages for TEDS:

1) Transducer contains data sheet information

2) No connection to PC is required

3) It can be used with many measurement points and with frequency changing configurations.

4) Makes measurements faster

5) Compactable with any kind of network and is not vendor specific

3 RELATED WORKS

There are many papers that propose methods for management of sensor networks. Sensor networks can be managed using Simple Network Management protocol. There are so many other protocols such as CMIP which is more effective in network management but SNMP is more simple and easy to implement.

There are many approaches in management of sensor networks using SNMP based MIB [7]. They are considering the overhead in the network. LiveNode Non-invasive Context-aware and modular Management (LiveNCM) is a wireless sensor network management tool which is divided in to two parts one is centralized on the fixed network structure and another one, distributed on each node. Each part introduces the concept of non-invasive context aware to reduce data exchanges and diagnoses the wireless sensor node state with few messages. LiveNMC is based on Live node platform to validate energy consumptions [13]. The main objective is to minimize the energy consumption by reducing the message exchanges. SNMP-based smart transducer interface module (STIM) is economical and scalable solution for sensor networks. It provides a transducer independent network accessible interface, which is useable to formalize the control of devices with different functions [2]. This MIB contains metadata, Meta identification, channel identification, channel, calibration, and calibration identification of TEDS information. The Entity MIB developed in1996 uses single agent to manage multiple instances of one MIB [7]. The Entity Sensor MIB contains a single group called the entitySensorValue group, which defines objects to convey current value and status of a physical sensor. This group contains a single table called entSensorTable, which provides a small number of READ-only objects. Management and Plug and Play of Sensor Networks using SNMP developed in 2011 is an extension to entity sensor combines TEDS to generate a new method for management end plug and play of sensor networks [10]. IEEE1451.4 is use to provide plug and play of sensor networks. It makes the sensor compactable with any kind of networks .The security aspects of the sensor by integrating SNMP is not implemented. IEEE 1451.4 TEDS provides the plug and play of instruments .It helps in the simplification of cable identification provides a class of templates categorizing common types of sensors. TEDS is a key feature that automates the process of inputting sensor related information. By using TEDS it is easy to identify and manage the sensor independent of the manufacturers. This makes the sensor SNMP compatible. IEEE1451.4 will reduce the challenges associated with the sensor configurations [11]. The entity sensor MIB can be extended to accommodate the sensor information .There is Template25 TEDS table for Template ID=25 and Template 36 TEDS table for Template ID=36 which uses Entity sensor MIB concept.

3.1 Skipjack Cryptographic Algorithm

Skipjack is a cryptographic algorithm used in wireless sensor networks. Here the input to the algorithm is the response send by the agent to the manager. It consists of executing two shift register algorithms such as RuleA and RuleB. To minimize memory for storage of data , we can use exactly as many bytes for the expanded key as there are in the user key.It is highly memory efficient algorithm compared with other sensor network encryption algorithm. It also has advantages like less time consumption and highly energy efficient [9]. It can be operated in several modes, but we chose to implement the basic ECB mode (Electronic CodeBook). This mode does not mess with the key schedule. The SkipJack algorithm takes an 80 bit key which is broken up into 10 bytes and four of which are used per round.Skipjack performs 32 rounds, in which 8 rounds for RuleA ,8rounds for RuleB, then perform the same steps once more. In each round 64bit plain text is subjected to permutation and after that 16 bit of it is through a substitution function (G) . This G function uses an 8 bit static substitution table (the F table) and a Feistel network to scramble the input bits further. During the decryption the functions are reversed.

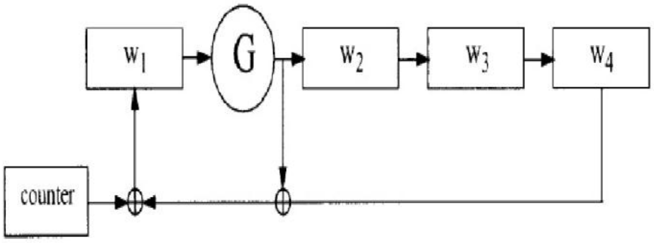


Fig 3: Rule A

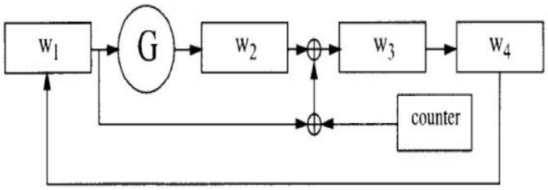


Fig 4: Rule B

4 PROPOSED MODEL

3.1 Design Considerations

The SNMP MIB is used to store the details regarding the sensor related information. The main aim is to enhance security aspects of SNMP, integrating with the sensor network management. The primary goal in sensor network is to minimize the energy usage by minimizing the messages. SNMP V3 provides two types of security models User Security model and Transport Security Model. But the security provided by the protocol is not much efficient when we integrate it with the sensor networks. So here we are proposing skipjack cryptographic algorithm for improving the security of the whole network [7].

MIB is first created by using MIB editor utilities provided by the webNMS SNMP C agent. After generating the MIB design next step is to compile MIB using the tool kit. Then the Generic code can be modified based on the user requirements. Once the management system is ready next step is to provide integrated security. The security is ensured using cryptographic method. The data send by the agent is encrypted using skipjack algorithm and is decrypted at the manager system. Here we use skipjack algorithm for ensuring security in the network. The algorithm is implemented using SNMPV1.Here we uses Electronic codebook mode cryptographic method. In this method the plain text is divided n to many blocks and each block is encrypted separately. At the receiver side separate decryption is done for each block. The figure for Electronic Codebook encryption is as shown below:

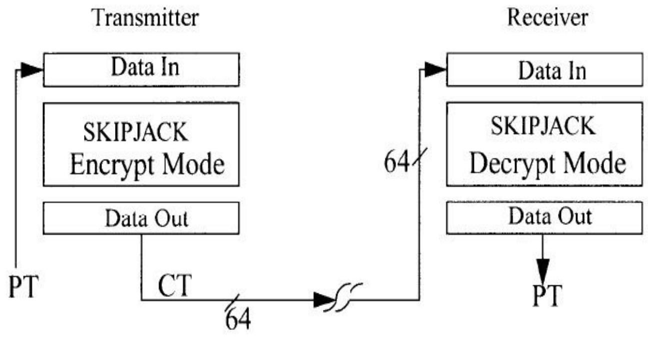


Fig 6: CodeBook mode diagram

PT -Plain Text (Messages/Responses send by the agent)
CT - Cipher Text
Here the transmitter is the agent process and Receiver is the manager.
The response messages send by the agent is encrypted by dividing the messages in to block of data and each block is termed as a word (w). Then each word is encrypted separately and is send to the manager system. At the manager side the decryption of each word is done and the words are combined to get the actual message [16].

4.2 Specification

1) Notations and Terms
V": Set of all n bit values.
Word: an element of V^{16} ;a 16 bit value
Byte: an element of V^{8}
W^i : word in the i'th step
G: substitution function
F-table: static table used by G function for substitution.

4.3 Structure

SKIPJACK encrypts 4-word (ie.8bytes) data blocks by alternating between two stepping rules A and B [9].

Rule A:

a. G Permutes w1
b. The new w1 is xor of the G output , the counter , w4
c. Words w2 and w3 shift one register to the right; ie, become w3 , and w4 respectively
d. The new w2 is the G output
e. The counter is incremented by one

Rule B:

a. G permutes w1
b. Permuted output is taken as the input to w2
c. W2 is xor with xor of (w1,counter) and is given as the input of w3
d. Output of w3 is given to w4
e. The new w4 is w1 input
f. Counter is incremented in each step

4.4 Stepping sequence

a. Encryption

- The input is w^0_i , $1\leq i \leq 4$ (k=0)
- Start the counter at 1
- Step according to ruleA
- Step according to RuleB
- Step 8 more times
- Return to RuleA for next 8 steps
- Return to RuleB for next 8 steps
- Counter incremented by one after each steps
- The output is W^0_i , $1\leq i \leq 4$

b.Decryption

- The input is W^{32}_i , $1\leq i \leq 4$ (k=32)
- Start the counter at 32
- Step according to RuleB^{-1} to next 8 steps
- Step According to RuleA^{-1} and 8 more steps
- Return to RuleB^{-1} for next 8 steps
- Return to RuleA^{-1} for next 8 steps
- Counter decremented by one after each steps
- The output is W^0_i , $1\leq i \leq 4$

4.5 G-permutation

The cryptographic variable-dependent permutation G on V^{16} is a four round feistel structure [9]. The round function is a fixed byte substitution table which will be called the F-table. Each round of G also incorporates a byte of cryptographic variable.

a. Recuresively : G^k (w=g1|| g6)=g5||g6 where $g_i=F(g_{i-1}$ XOR $cV_{4k+i-3})$ XOR g_{i-2}
b. Schematically:

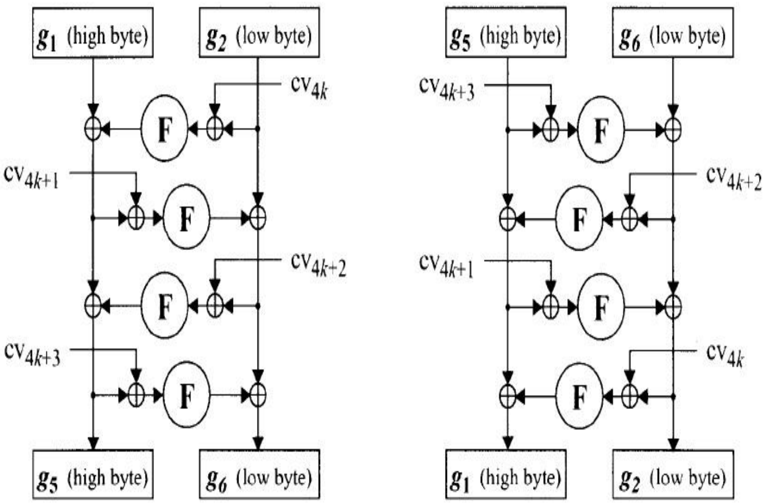
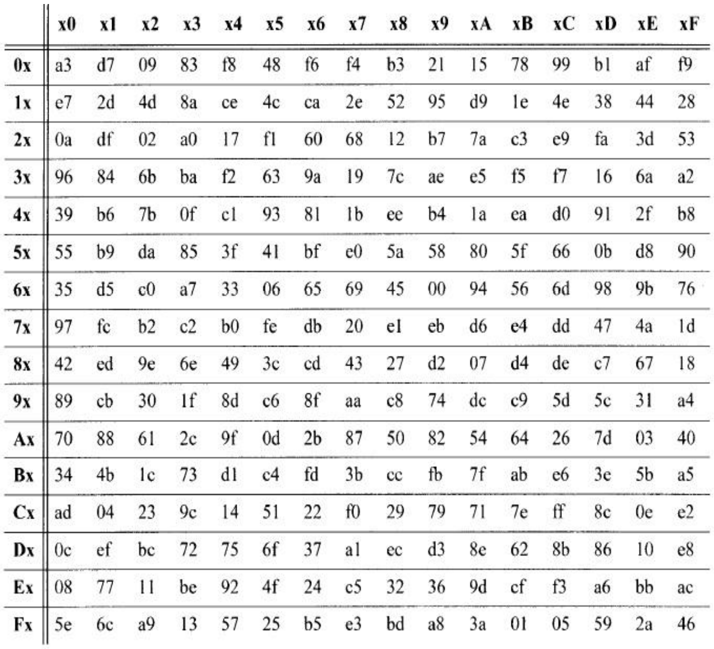


Fig 7: G-permutation diagram

The cryptographic variable is a 10 byte long and is used in its natural order. So the schedule subscripts given in the definition of the G-permutation are to be interpreted mod-10.

c. F-table:
The SKIPJACK F-table is given below in hexadecimal notation. The higher order 4 bits of the input index are the row and the lower order 4 bits index is the column [9]. Table1 is given below:

Table 1:F-Table



	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	a3	d7	09	83	f8	48	f6	f4	b3	21	15	78	99	b1	af	f9
1x	e7	2d	4d	8a	ce	4c	ca	2e	52	95	d9	1e	4e	38	44	28
2x	0a	df	02	a0	17	f1	60	68	12	b7	7a	c3	e9	fa	3d	53
3x	96	84	6b	ba	f2	63	9a	19	7c	ae	e5	f5	f7	16	6a	a2
4x	39	b6	7b	0f	c1	93	81	1b	ee	b4	1a	ea	d0	91	2f	b8
5x	55	b9	da	85	3f	41	bf	e0	5a	58	80	5f	66	0b	d8	90
6x	35	d5	c0	a7	33	06	65	69	45	00	94	56	6d	98	9b	76
7x	97	fc	b2	c2	b0	fe	db	20	e1	eb	d6	e4	dd	47	4a	1d
8x	42	ed	9e	6e	49	3c	cd	43	27	d2	07	d4	de	c7	67	18
9x	89	cb	30	1f	8d	c6	8f	aa	c8	74	dc	c9	5d	5c	31	a4
Ax	70	88	61	2c	9f	0d	2b	87	50	82	54	64	26	7d	03	40
Bx	34	4b	1c	73	d1	c4	fd	3b	cc	fb	7f	ab	e6	3e	5b	a5
Cx	ad	04	23	9c	14	51	22	f0	29	79	71	7e	ff	8c	0e	e2
Dx	0c	ef	bc	72	75	6f	37	a1	ec	d3	8e	62	8b	86	10	e8
Ex	08	77	11	be	92	4f	24	c5	32	36	9d	cf	f3	a6	bb	ac
Fx	5e	6c	a9	13	57	25	b5	e3	bd	a8	3a	01	05	59	2a	46

5 CONCLUSION

The management and plug and play of sensor networks using SNMP is already implemented. Here we provide security aspects of sensor networks by integrating SNMP with SKIPJACK encryption algorithm for ensuring security in the network. It is an energy efficient algorithm so that is compatible with sensor network.

REFERENCES

[1] Management and Plug and Play of Sensor Networks Using SNMP Syed Alamdar Hussain, Student Member, IEEE, and Deniz Gurkan, Member, IEEE, IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 60, NO. 5, MAY 2011

[2] J. D.Case, M. S. Fedor, M. L. Schoffstall, and J. R. Davin, A Simple Network Management Protocol, (SNMP), DDN Network Information
Center, SRI Int., May 1990, RFC 11 57.

[3] J. Case, R. Mundy, D. Partain, and B. Stewart, Introduction to Version 3 of the Internet-Standard Network Management Framework, Apr. 1999, RFC 2570.

[4] J. Case, K. McCloghire, M. Rose, and S. Waldbusser, Introduction to Version 2 of the Internet-Standard Network Management Framework, Apr. 1993.

[5] F. Kastenholz, SNMP Communications Services, Oct. 1991, RFC 1270.

[6] M. Rose and K. McCloghire, Structure and Identification of Management Information for TCP/IP-Based Internets, May 1990, RFC 1155.

[7] K. McCloghire and M. Rose, Management Information Base for Network
Management of TCP/IP-Based Internets: MIB-II, Mar. 1991, RFC 1213.

[8] Int. Org. Standardization, Information Processing Systems—Open Systems Interconnection—Specification of Abstract Syntax Notation One (ASN.1), Int. Std. 8824, Dec. 1987.

[9] SKIPJACK and KEA Algorithm specification ,US national security agency, Version 02,1998

[10] S. Gumudavelli, D. Gurkan, and R. Wang, "Emulated network of IEEE 1451 application with multiple smart sensor reports," in Proc. IEEE Sensor Appl. Symp., New Orleans, LA, 2009, pp. 304–308.

[11] IEEE, IEEE Standard for a Smart Transducer Interface for Sensors and Actuators—Network Capable Application Processor (NCAP) Information Model, IEEE Std. 1451.1, 1999.

[12] IEEE, IEEE Standard for A Smart Transducer Interface for Sensors and Actuators—Mixed-Mode Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats, IEEE Std. 1451.4, 2004.

[13] A. Jacquot, J.-P. Chanet, K. M. Hou, X. Diao, and J.-J. Li, "A new approach for wireless sensor network management: LiveNCM," in Proc. NTMS, Nov. 2008, pp. 1–6.

[14] B. Scherer, C. Toth, T. Kovacshazy, and B. Vargha, "SNMP-based approach to scalable smart transducer networks," in Proc. 20th IEEE IMTC, May 2003, pp. 721–725.

[15] K. McCloghrie and A. Bierman, Entity Management Information Base, Oct. 1996, RFC 2037.

[16] SkipJack Algorithm Alexander Dean Jonathan Johnson February 15, 2012