BLOCKING OF EAVESDROPPING ATTACK IN THE INDUSTRIAL WIRELESS SENSOR NETWORKS

G.Sivaramasubramanium¹, G.Amsaleka², S. Aswin Paul², A.Gokulavani², S.Keerthana² Assistant Professor¹, Final Year Students², Department Of ECE, Erode Builder Educational Trust's Group of Institutions, Kangayam, Tirupur.

Abstract:

Blocking of Eavesdropping attack from data hacking process has attracted considerable attention from the communities of privacy security and protection. In existing system, all attackers are not based upon IP monitoring system and there is no noise aided security to collapse the hacker. So it is easy to crack the data within a short duration. In the proposed system we include IP monitoring system and secret keys to hide the data. In this method Advanced Encryption Standard (AES) algorithm is used for bitwise encryption technique which will be secure for encryption. So it is very complex to hack the encrypted data. Encrypted hidden data is generated using data hiding key. So, it will be very easiest method to block the eavesdropper.

Keyword: Eavesdropping attack, IP monitoring method, AES algorithm, Encryption technique and cryptographic key.

1.Introduction:

Wireless network security issues continue to make current headlines attention has been drawn away from the fact that wired networks are often affected by many of the same weakness. Eavesdropping attacks are insidious, because it's very difficult to know where they are occurring. So we use IP based monitoring system to get the warning signal to block the attacker from the predefined authenticated node design. Cryptographic encryption technique is used to encrypt the plaintext and AES algorithm is used to protect the encrypted data using secret key generation and to send information to destination safely.

Wireless sensor networks (WSNs) were initially motivated by the military for battlefield surveillance [1], and now are further developed for various industrial applications such as the assembly line monitoring and manufacturing automation for the sake of improving the factory efficiency, reliability, and productivity [2], [3], which are referred to as the industrial WSNs [4]-[6]. In industrial WSNs, due to the broadcast nature of radio propagation, the wireless medium is open to be accessed by both authorized and unauthorized users, leading WSNs to be more vulnerable to the eavesdropping attack than wired sensor networks , where communicating nodes are physically connected with wire cables and a node without being connected is unable to access for illegal activities. Therefore, it is of importance to investigate the protection of industrial WSNs against the eavesdropping attack.

2. Eavesdropping Attack:

Eavesdropping is the unauthorized real time interception of a private communication, such as a phone call, instant message, video conference or fax transmission. Eavesdropping is an electronic attack where digital communications are intercepted by an individual whom they are not intended, it is the act of intercepting communications between two points. In the digital world, Eavesdropping takes the form of sniffing for data in what is called network eavesdropping. A specialized program is used to sniff and record packets of data communications from a network and then subsequently listen to (or) read using cryptography tools for analysis and decryption.

ISSN 2395-695X (Online) International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Actual eavesdropping that is the simple act of listening to the other people talk without then knowing it, can be done using current technology such as hidden microphones and records. Hacking into devices such as IP phones is also done in order to eavesdrop on the owner of the phone by remotely activating the speaker phone function. For example, "e-mail" if the sender has not encrypted the e-mail message and has not used digital signature the attacker can exploit security loop holes on the network to launch the eavesdropping attack.

3.Advanced Encryption Standard Algorithm (AES):

Advanced version of data encryption and it is a symmetric key encryption algorithm. To overcome the disadvantage of DES algorithm we move to AES. AES cipher has block length of 128 bit. Key size is independently specified to 128,192, or 256 bits. AES parameters N_b = number of columns in the state, N_k = number of 32 bit words in the key $N_{r=}$ Number of rounds. AES methods convert to state array, transformation, key expansion.

Encryption technique: Encryption is a great defense against eavesdropping. By only using applications and systems which use strong encryption, you can make an attacker's life far more difficult. But it isn't a panacea, for a couple of reasons. First, we continue to see a dual pronged attack against encrypted data. Faster PC's reduce the time of an attacker needs to crack a password, cracking technologies, such as rainbow tables can reveal password in seconds.

4.Cryptographic Key:

The term Cryptography means "secret writing". An encryption algorithm transforms the plain text into cipher text, a decryption algorithm transforms cipher text into plain text. Sender sends the information in the form of plain text it is encrypted as the cipher text and decrypted as a original message called plain text to the receiver. Cipher is used to different categories of algorithms in cryptography.

Cryptography is divided into two groups: Symmetric key and Asymmetric key. Symmetric key is a secret key and asymmetric key is a public key. In symmetric key cryptography the same key is used by the sender and receiver. In asymmetric key different key is used by the sender and receiver.



Sink nodes

6.Software requirements:

Operating System : Windows

Simulator Tool : Net Beans 7.2.1

Language : Java

Development Kit : JDK1.7

Platform : Independent

ISSN 2395-695X (Print)

Vol. 2, Special Issue 10, March 2016

7.Simulation output :

In this project, we are using a NetBeans IDE 7.2.1 software for designing a layouts. The designing of layouts includes labels, text fields, text areas, buttons and panels. The layouts for Sensor node, Monitoring node, Sink nodes and Hacker node were designed and coded by "JAVA" language.

SENSOR NODE

5		N .	\$												_ □ >	<
Recycle Bin	NetBeans IDE 7.4	Snake-mae		Industr	ial Wire	less Sens	or Netwo	orks in t	the Pres	sence of	Eavesd	ropping	Attack			
							SENSO	R				File A	ttributes	[
My	WaterPump	LoadBalane -RULL		I	Р	19	2.168.1.	11		Connect		Docum	ent.txt		Client A	
1		w h		E A Maria	Turk Da		a Dur		Salit	Deslasta	3	Ved Jan	27 15:15:42 IST	T 2016	192.168.1.11	
Adobe	WaterPump	screen		=: \New	Text Do	cument.tx	GT Brow	vse 2	sput	Packets	-				Client B	
Reader 9				int ne }	noOfitems w KMean(k,	= input.nextl , noOfitems)	int(); ;				Â	•			192.168.1.11	
2				publi	ic static int a sum = 0;	average(Arra	yList <intege< td=""><td>r> list) {</td><td></td><td></td><td></td><td>Clien</td><td>e Clients it A</td><td></td><td>Client C</td><td></td></intege<>	r> list) {				Clien	e Clients it A		Client C	
Capture	geogra para			101 }	sum = sum	+ value;						Clien Clien	at B at C		192.168.1.11	
				}	um sum / II	st.size(),					¥	Chen				
oSSLSched	appcompa						_								Chent D	
lin	(No o	f Packets	for batch	1			KeyG	en	Sig	nOnData		Not Connected	
	jej			******	******D	ata Sign*	*******	*****								
ellimellrack.	. ksoap2-and			Batch Batch	1 - 0,00 2 - 0,00	UU.UY>306	SUeu8UUUY	UUURhU&2	:Uqu}UU=l	100001\$0						
				000 bX 0	0K00v:200	00 5 00W00	200 500 و0	10 A0L0[6 0	10							
💨				Batch	3 - 0-00]]]]i #0u []]	010004kwi	#0 J 0000m	100B00Q	F00000ir0{	00					
Mozilla Firefox	New															
								-		Clear			Send			
CRESH		<u>e</u> [~		<u></u>	<u>S</u>	S	<u></u>	<u></u>		W			

MONITOR NODE:

0	LoadBalancer - NetBeans IDF 7.4		×
File Edit View Navigate			Q → Search (Ctrl+I)
Projects × Files S	Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack		
New ClientA	MONITERING NODE	Client A	Tabbed Pane
ClientC	Server Not Connected Batch Received	Not Connected	Desktop Pane
MainGr MainGr Router	Packets to Client	Client B	i Button i ⊂ Check Box
ShowM	Client A Batchs	Not Connected	©_Button Group ↓ s ×
Test Packages Joraries Test Libraries	Client B Batchs	Client C	on EXIT_ON_CLOSE
[JFrame] - Navigator ×		Not Connected	
	Chent C Batchs	Client D	Ø
	Client D Batchs	Not Connected	
		Hacker	
		Not Connected	
			~
		LoadBalancer (run) #6 running	📓 (5 more) 1 1 INS
			😽 💭 ♠) ENG 14:34 03-03-2016

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

CONNECTED DETAILS:

0	LoadBalancer - NetBeans IDF 7.4		- 🗆 🗡
File Edit View Navigate	al de la companya de	- • ×	Q ▼ Search (Ctrl+I)
Projects × Files S	Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack		
New ClientA	MONITERING NODE	Client A	Tabbed Pane
ClientC	Server 192.168.1.11 Batch Received	192.168.1.11	Desktop Pane
MainGr	Packets to Client	Client B	©E Button ≅− Check Box
ShowM	Client A Batchs	192.168.1.11	S × −
 Test Packages Libraries Test Libraries 	Client B Batchs	Client C	on EXIT_ON_CLOSE V
[JFrame] - Navigator × Form ClientB	Cline C Burke	192.168.1.11	rd 🖉
. [JFrame]	Cirent C Dattas	Client D	0
	Client D Batchs	Not Connected	
		Hacker	ndBalancer (run) #6 × ∢ ⊦
		192.168.1.11	ĥ
			* *
		LoadBalancer (run)	🕅 (5 more) 1 1 INS
	2 📑 🚯 🖊 🗊 👙 👙 👙 👙	- 🛚	(☐ (1)) ENG 14:40 03-03-2016

NODE 1:

RECEIVE THE PACKET

		_ 0 ×
File Edit View Navigate Source Re		2 - Search (Ctrl+I)
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack	
Projects × Files Services	NODE-I	Tabbed Pane
ClentC java		E Scroll Pane
ClientD.java	IP 192.168.1.11 Disconnect ************************************	🔚 Desktop Pane
🔂 Hacker.java	Batch 1 Verification true	Layered Pane
- 🔂 MainGraph.java	Clear Buffer Batch 2 Verification true	
MainGraph1.java	Batch 3 Verification true	OK Button
Router.java		III − Check Box
ShowMessage.java		🖁 🗌 Button Group 🗸 🗸 🗸
🗟 ShowMessage 1. java	Pasand Batch	- s ×
images.jpg	Resenu Datch	Events Code
Image: Test Packages		^
Doraries		on EXIT_ON_CLOSE 🔻
Eorm ClientB		
Dther Components	Packets Received	d V V
. [JFrame]	public static init average(ArrayListstatieger> iist) {	0
	int sum = 0;	-
	for (Integer value : list) {	
	sum = sum + value;	-
		dBalancer (run) #6 🗙 👍 🕞
	return sum / list.size();	^
	3	
	DOWNLOAD	
		U
		(5 more) 111 mm
		14.4
	👬 🚯 📥 💭 🖆 🖆 🗳 🗳 🗳 💆 📥 🔸	14:41 ()) ENG 03-03-2016

Vol. 2, Special Issue 10, March 2016

NODE2:

RECEIVE THE PACKET

			- 🗆 🗡
File Edit View Navigate Source Refactor Ru	ار. ۱	Q	Search (Ctrl+I)
한 🔁 😫 🖣 🦻 🥐 🛛 <default< th=""><th>Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack</th><th></th><th></th></default<>	Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack		
Projects × Files Services		te ×	_
🖻 🖷 New	SINK NODE-II	ing Containers	^
ClientA.java		nel	Tabbed Pane
ClientB.java		lit Pane	Scroll Pane
CientC.java	IP 192 168 1 11 Disconnect	ol Bar	🔁 Desktop Pane
Hacker java	Batch 1 Verification true	ternal Frame	Layered Pane
MainGraph.java	Clear Buffer Batch 2 Verification true	ing Controls	
🔂 MainGraph 1. java	Batch 3 Verification true	bel	OK Button
- Router.java	Resend Batch	ggle Button	I → Check Box
Server.java		dio Button	8 Button Group
ShowMessage.java		mal Preparties	× _
images.ipg	**************************************	whice Rinding	Fuents Code
🗈 🊡 Test Packages		ardies binding	Events Code
🕀 🍒 Libraries		ItCloseOperation	EXIT ON CLOSE -
🗄 🎽 Test Libraries	Packets Received		
[JFrame] - Navigator ×		r Properties	
Form ClientB	import static lava lana Math abs:	sOnTop	
Other Components	import and jural languint.	sOnTonSunnorted	V *
	import invo util Collectors:	ne]	6
	import invaluti Sconener.		
	import jureanneseement,		
	nublic class KMeen J		-
		n) #5 × LoadB	Jalancer (run) #6 🛛 🖂 🖂
	ina lu.		^
	DOWNLOAD		
			¥
			g (5 more) 1 1 INS
		- 18 19	14:41 (1) ENG 03-03-2016

NODE 3:

NODE 3:				
RECEIVE THE PACKET			\sim	
0	4		×	- 🗆 ×
File Edit View Navigate Source Refactor Run			Q.• Sea	arch (Ctrl+I)
Projects X Files Services	Industrial Wireless Sensor Networks in the Prese	nce of Eavesdropping Attack	te X	
e			ving Containers	^
ClientA.java	SINK NO	ODE-III	anel	Tabbed Pane
CientS.java			plit Pane	Scroll Pane
ClientD.java			bol Bar 🖉	J Desktop Pane
Hacker.java		******************** Packet Verification ******************	iternal Frame	Layered Pane
MainGraph1.java		Batch 1 Verification true	abel DK	Button
Router.java	IP 192.168.1.11 Disconnect	Batch 2 Verification true	pagle Button 🛛	- Check Box
Server.java	Clear Buffer	Batch 3 Verification true	adio Button 8:	Button Group
ShowMessage.java	Cital Buller		mel Preperties X	
images.jpg	Resend Batch		erties Binding F	Events Code
🗈 🎧 Test Packages		**************************************	perties	A
🕀 🔓 Libraries			ItCloseOperation EX	IT_ON_CLOSE 🔻 🛄
EF Dest Lorares				
[JFrame] - Navigator ×	Packets Received		er Properties	1
Other Components			sOnTonSupported V	· · · ·
🗈 - 🛅 [JFrame]	import static java.lang.Math.abs;	n	me]	0
	import java.util.ArrayList;			
	import java.util.conections;			
	import java.arn.ooannet,			-
	public class KMean {		n) #5 × LoadBala	ncer (run) #6 🛛 🖂 🕞
				^
	int k;	Y		
	DOWNL	LOAD		
				~
			(5	more) 1 1 INS
🙆 🙆 🚞	🚯 📐 🕥 ዿ 👙 🔮		- 😼 🕀 🐠	ENG 14:44 03-03-2016

Vol. 2, Special Issue 10, March 2016

8.EXPECTED OUTPUT:

HACKER INFORMATION VIEW MONITER NODE

0	LoadBalancer - NetBeans IDF 7.4		- 0 ×
File Edit View Navigate			Search (Ctrl+I)
Projects × Files S	Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack		
New ClientA	MONITERING NODE	Client A	Tabbed Pane
ClientC	Server 192.168.1.11 Batch Received 6	192.168.1.11	En Scroll Pane
MainGr MainGr Router Server	Packets to Client	Client B	© Button ₽− Check Box
ShowM	Registration Response Message	192.168.1.11	S_Button Group
Instructions	Hacker Connected	Client C	on EXIT_ON_CLOSE ▼
Form ClientB	Ok Client C Batchs	192.168.1.11	
û		Client D	Ø
	Client D Batchs	Not Connected	-
		Hacker	dBalancer (run) #6 × 4 > 1
		192.168.1.11	
			· · · · · · · · · · · · · · · · · · ·
		LoadBalancer (run) #6	running (5 more) 1 1 INS
			▲ 🙀 🖓 🔛 I()) ENG 03-03-2016

HACKER NODE BLOCK

Recycle Bin NetBeans IDE Snakern 7.4		
Ny Bluetoo	Hacker node	
Addie WaterPump serce	Router IP 192.168.1.11 Connect Disconnect	
Camero Capitore	Registration Response Message Access Denied You not Have a ANONYMOUS Client	
assistinati. apprompt.	Ok	
ettinettedk (soog2-and		
🔐 🙋 🥭	🚝 🚯 📥 💭 ዿ ዿ ዿ 🔮 🗶	▲ 隆 🐏 ⊌) ENG 14:38 03-03-2016

9.CONCLUSION:

In this paper, we propose an AES (Advanced Encryption Standard) algorithm for text encryption and decryption of wireless transmissions from sensor to the sink nodes. AES algorithm is more secure to transfer files from sensor to sink nodes. And also IP monitoring is provided to block the Eavesdropping attack. IP provides the end to end communications between nodes. By IP monitoring we can identify what are all the nodes are connected to the server and how much amount of packets are have been receiving to the sink nodes from sensor. We can easily block the attacker by IP monitoring.

10.REFERENCE:

[1]. C. E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, 1949.

[2]. W. Shen, T. Zhang, F. Barac, and M. Gidlund, "PriorityMAC: A priorityenhanced MAC protocol for critical traffic in industrial wireless sensor and actuator networks," IEEE Trans. Industrial Informatics, Feb. 2014.

[3]. J.-C. Wang, C.-H. Lin, E. Siahaan, B.-W. Chen, and H.-L. Chuang, "Mixed sound event verification on wireless sensor network for home automation," IEEE Trans. Industrial Informatics, vol. 10, no. 1, pp. 803-812, Feb. 2014.

[4]. T. M. Chiwewe and G. P. Hancke, "A distributed topology control technique for low interference and energy efficiency in wireless sensor networks," IEEE Trans. Industrial Informatics, vol. 8, no. 1, pp. 11-19, Feb. 2012.

[5]. P. T. A. Quang and D.-S. Kim, "Enhancing real-time delivery of gradient routing for industrial wireless sensor networks," IEEE Trans. Industrial Informatics, Feb. 2012.

[6]. M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," IEEE Trans. Industrial Informatics, vol. 9, no. 1, pp. 277-293, Feb. 2013.

[7]. "Amit Kumar Mishra", "Text and Image Encryption Decryption Using Advanced Encryption Standard", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3, May -June 2014.