Proc. of Int. Conf. on Advances in Communication, Network & Computing, CNC

The RSSI based Key Distribution Approach in Wireless Sensor Network and it's Application

Mr.Rushi Trivedi[1] and Mr.Chetan Kamani[2]
[1-2]C.U.Shah Government Polytechnic, Surendranagar, India
Email: rt1764@gmail.com, chetan.kamani@yahoo.com

***Abstract*—It is required to maintain privacy of critical information when it is sent over the channel. The wireless sensor network can be used in defense applications like detecting intrusion ,enemy tracking and protection against force tracking. Wireless sensor network is made of distributed sensor nodes which are connected to each other. Nodes have limited resources for computation, transmission and other activities. But this network is vulnerable to various kinds of security threats like eavesdropping, node capturing and man in middle attack. To ensure security of critical information over communication channel , messages must be encrypted. This scheme will use the inherent parameter of a wireless sensor network. This will improve performance in terms of resource consumption for resource constrained network.**

***Index Terms*— Key distribution, Encryption, Network security, Wireless Sensor Network.**

I. INTRODUCTION

The Wireless Sensor Network is made of very small cheap and low power devices. It is a very special type of ad-hoc network. This network highly dependent on the functionality that the user wanted to do from a network, all nodes in the network together want to achieve that functionality. Depending upon the application, all the nodes in the network may be same or maybe not. If all nodes in the network have to perform a same functionality than that type of a network is called a homogeneous network If nodes have different hardware design; or different roles than that type network is called a heterogeneous network. In Most of Wireless Sensor Network Application, Data is gathered by the sensor nodes and will be transmitted to sink node or base node. For an example in the wildlife monitoring system or temperature sensing application, it may not be critical to transfer data as an unencrypted data, as normally the third party are not interested in such kind of data, But there are many other application where data is critical and the confidentiality and integrity of data is important. for an example military application, theft detection, home security applications. The wireless sensor network security level is depend upon the application, Like normal network there is no common security framework is available that will be directly applicable to all the types of application. To achieve a basic security fundamental of the network. It must have the secure key distribution infrastructure. Based on that we can achieve confidentiality, integrity and authentication.

II. PROPOSED APPROACH

Fundamental thinking here is that we can use an inherent attribute of the packet for the key generation of wireless sensor network. We will use received signal strength as a one of the parameters for a unique key

Grenze ID: 02.CNC.2018.9.1

distributed among the nodes. We will focus on possible solutions for the proposed key distribution scheme.
Assumption: Nodes are deployed randomly.
Protocol Design: For Secure communication with the nodes ,base station will select an elliptical curve over a finite field GF(P). it will release a base point P of large order Q.Q must be a prime number. it will generate random number r as its private key. PR € GF(P).Now, master public key will be PU= r * P. Base Station will broadcast its public key to all nodes. For Securely Share Symmetric key all nodes will generate their own public-private key pair based on finite field GF(P).For Node i, ri € GF(P) ,PUi = ri * P.
Step 2:In Neighbourhood Discovery Every node will broadcast their public key with Hello packet. After Neighbourhood discovery, each node has a list of all its neighbourhood nodes with a public key and RSSI value.

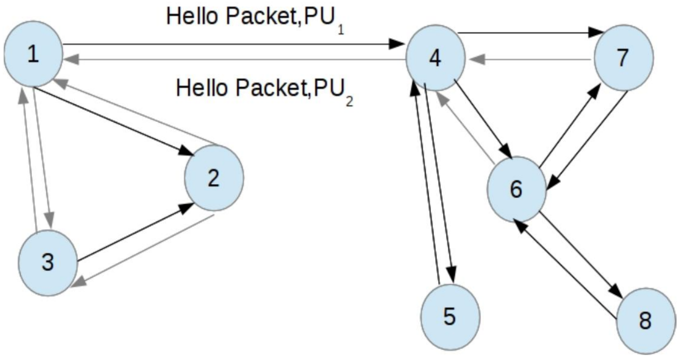

Fig 1. Neighbourhood Discovery

As, now we are considering that RSSI value may be varied After neighbourhood discovery, Each Node will maintain the following format of the table.
Step 3: Secure Communication Establishment
Now consider Node 1 want to communicate with Node 4. Node 1 will send packet to Node 4, In which it will encrypt data using Node 4's Public Key. First packet is send from Node 1 to Node 4.Packet contains following value.

TABLE II. PACKET SENT BY NODE1 TO NODE 4

RSSI	K1	K2

Node 4's RSSI value which is stored in the table.it will generate random number K1;K2
Node 4 will compute the value R = ((K1 -1) *(K2-1)) * sqrt(K1*K2)/(K1 -K2).It will choose one prime number from range(0,R).As it received a packet from Node 1,it will extract the RSSI value from the packet. It will update the table put it in RSSI2 Now it will create Packet with following Data, encrypted it with Node 1’s Public Key. The updated table For Node 1 and Node 4. Now Node 1 and Node 4 has the following values R;RSSI1;RSSI2.Node can compute key based on these three inputs using any cryptographic function.
K = Function(R;RSSI1;RSSI2) This Key K can be used for symmetric key

III. APPLYING KEY DISTRIBUTION ALGORITHM

After having a Key Distribution mechanism, the encryption algorithm plays a key role in ensuring the certain level of security in the network. we need to find a suitable encryption algorithm for the wireless sensor network. The Main aspect to the use of encryption algorithm is achieved confidentiality in the network.
If we analyze the history of encryption algorithm, we realize that many encryption algorithms evolve over time, cracked over time. Most of the encryption algorithm is secure for a certain period of time.
Most of the encryption algorithm is cracked due to error-prone design or it will be cracked in future using brute-force approach with high computational power. Most common approach is that increase the key size for encryption algorithm as computational power increase. Ordinary encryption algorithm and their design is unsuitable for the wireless sensor network. Let us analyze few encryption algorithms and their compatibility with our key distribution mechanism and wireless sensor network.

IV. ONE TIME PADDING

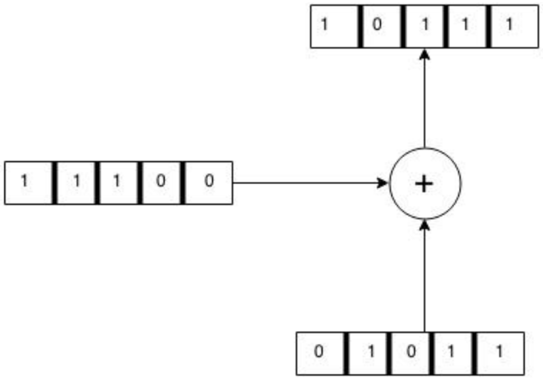

Fig 2.One Time Padding

A. The benefits of one time padding

It is cryptanalytically unbreakable. It is very fast, required very less computational power. In one time padding key length is same as data size, for sensor network packet size 29 bytes compare to Ethernet packet it is very less.

B. Requirements of One Time Padding

The key size must be same as plain text.The key generated by algorithm must be uniformly distributed and random.Each encryption operation must use unique key.

V. INTEGRATION OF RSSI BASED KEY DISTRIBUTION AND ONE TIME PADDING

Why RSSI Based Key Distribution is suitable for One Time Padding For Implementing one time key padding properly in the network, The key generated by the algorithm must be truly random. It is already proven for generating true randomness in the network, we can use bit errors in the sensor network. RSSI based key distribution used RSSI value for generating a random key which is truly dependent on the noise and bit errors in the network. Step 1: Assuming all the nodes in the network are using RSSI based key distribution algorithm. They performed key distribution based on algorithm. After key distribution, each node has a following data.(R,RSSI1,RSSI2).Step 2:Node will compute seed value based on above value.
seed = ((R - RSSI1) * (R + RSSI2)).Step 3: Node 1 and Node 2 has a same seed value ,the seed value will be given to the pseudo random number generator. Step 4,for every transmission it will use one random number as the key which is generated by the Pseudo random Number generator. Both the side key will be generated using PRNG for every transmission.

VI. RESULT

One time padding is compared with secure AES 128 bit symmetric key encryption. it is already analyzed that One Time Padding(128 bit) encryption operation efficiency is approximately three times better than AES(128 bit) encryption operation. It is due to the fact that the encryption operation depends on simple XOR operations. A XOR operation required only one clock cycle on the ATmega architecture when it is performed between registers. We are using micaz mote with 4.5V supply voltage andcurrent drawn 8mA for Active mode of processor.

TABLE II. SIMULATION PARAMETER

Simulator name	MATLAB
Number of Nodes	100
Deployment	RANDOM
Path loss propagation model	Free Space(N=2)
Energy Model	Micaz Motes

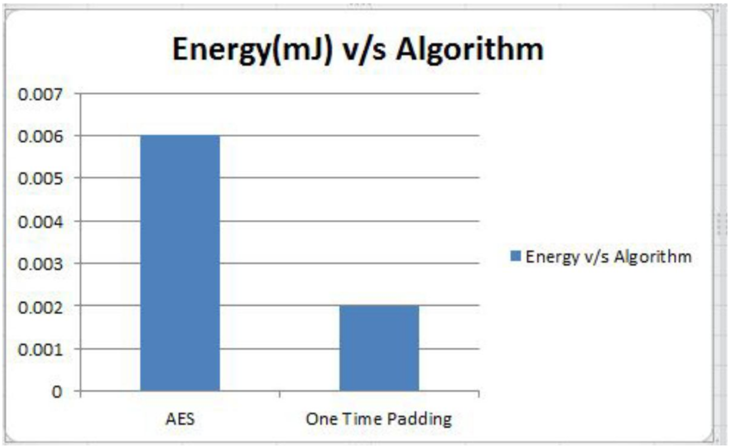

Fig 3. Energy consumption for one encryption operation

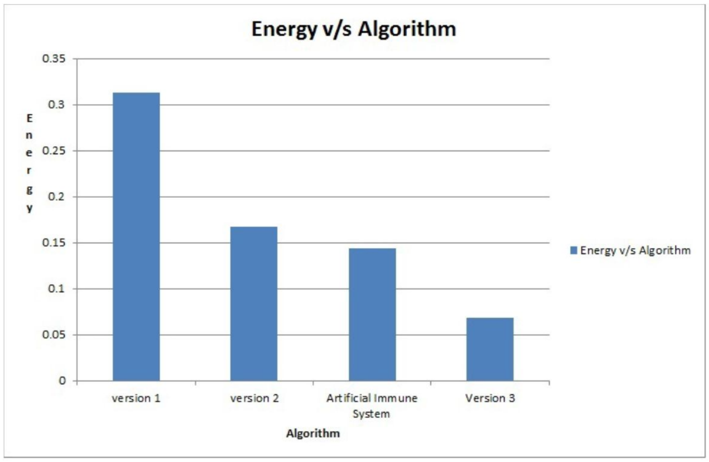

Fig 4. Energy consumption for key distribution algorithm

References

[1] Marcos A. Simplcio Jr., Paulo S.L.M. Barreto 1, Cintia B. Margi,Tereza C.M.B. Carvalho “A survey on key management mechanisms for distributed Wireless Sensor Networks“, Computer Networks Volume 54, Issue 15, 28 October 2010, Pages 2591-2612.

[2] Kumar, E. Sandeep, S. M. Kusuma, and BP Vijaya Kumar. "A random key distribution based artificial immune system for security in clustered wireless sensor networks." In Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on, pp. 1-7.

[3] Gupta, Rajat, Kaushal Sultania, Pallavi Singh, and Archit Gupta. "Security for wireless sensor networks in military operations." In Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on, pp. 1-6. IEEE, 2013.

[4] Karlof, Chris, Naveen Sastry, and David Wagner. "TinySec: a link layer security architecture for wireless sensor networks." In Proceedings of the 2nd international conference on Embedded networked sensor systems, pp. 162-175. ACM, 2004.

[5] Seo, Seog Chung, Hyung Chan Kim, and R. S. Ramakrishna. "A new security protocol based on elliptic curve cryptosystems for securing wireless sensor networks." In EUC Workshops, pp. 291-301. 2006.

[6] Büsching, F. and Wolf, L. "The Rebirth of One-Time Pads—Secure Data Transmission from BAN to Sink". IEEE Internet of Things Journal, 2(1), pp.63-71.

[7] Wander, A.S., Gura, N., Eberle, H., Gupta, V. and Shantz, S.C., 2005, March. Energy analysis of public-key cryptography for wireless sensor networks. In Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on (pp. 324-328).