International Journal of Engineering Research and Application www.ijera.com ISSN : 2248-9622, Vol. 6, Issue 9, (Part -5) Sepamber 2016, pp.99-103

RESEARCH ARTICLE OPEN ACCESS

WSN: An Effective Data Privacy Arrangement

Manmath Nath Dash[1] , R Subba Rao[2], Satya Sobhan Panigrahi[3]
[1,3]*Associate Professor, Department of Computer Science Engineering, Gandhi Institute For Technology (GIFT), Bhubaneswar*
[2]*Assistant Professor, Department of Computer Science Engineering, Gandhi Engineering College, Bhubaneswar*

ABSTRACT
Actually the full network level privacy is categorized into four sub parts: Identity privacy, route privacy, location privacy and data privacy, we need to provide privacy in the four categories. Achieving complete network level privacy is a cumbersome task due to the constraints imposed by the sensor nodes, sensor networks and Quality of issues.
In this paper,mainlyconcentratedonthedataprivacyforWSNs. Therefore I proposed encryption and randomnumber generation techniquesto provide efficient data privacyforWSNs.ForthatI am using the RSA algorithm which addresses those techniques. ThroughthisRSAalgorithmwecanprovideeffectivecomputation cost that is required to perform encryption and random number generation.
Keywords: Wireless Sensor Networks, Sensor Nodes, Privacy, Encryption, Random Number Generation, RSA Algorithm

I. INTRODUCTION

From the definition of [6], Wireless Sensor Networks (WSN) are devices that are composed of large number of small sensor nodes and each sensor node consists a simple processing unit (CPU), a memory unit for storage purpose, and sensing and communicationcapabilities.TheseWSNsworkonthe principle of Ad-Hoc networks. Each node is a transceiver .It means it can receive and transmit data.
TherearewidelyspreadingapplicationsofWSNsinsev eralareas especially in sensitiveareas.

- Someare"Disasterreliefapplications"[6]inwhic htheWSN is employed with thermal sensors, measuring th average temperature.Forexampleinaforest,automaticall yalarming the fire department if the temperatures get toohigh.
- Another field where WSNs could be applied is in military applications ,they could measuresomeimportantinformation for the army. In this case it is obvious that a certain level of security is required; therefore there is a need for encryption algorithms.
- Andthereareseveralotherapplicationfieldslikehe althcare,habitat-monitoring etc.

The need for encryption is always present, especially after the incident in which US Army surveillance airplanes, Predator MQ-1's, were not using any encryption algorithms for their surveillance video data [3]. The videos and images of territories under surveillance were monitored by Iraqi militants as well,by justusingasharewarewindowsapplication,satellitecar dreceiver and a satellite parabola dish[3].
In the following sections first the WSN requirements will be explained, and then the related work, network model and then the encryption method will be discussed.

The below fig. shows a model of wireless sensor network.

- In that the small squares shows the sensor nodes through which the information is passsed.It means these smallunitscontainsenergy,memory,andComput ationpower.hebigbrowncircleshowsthegateway sensornode.Itmeans it is like a base station for the smallunits.

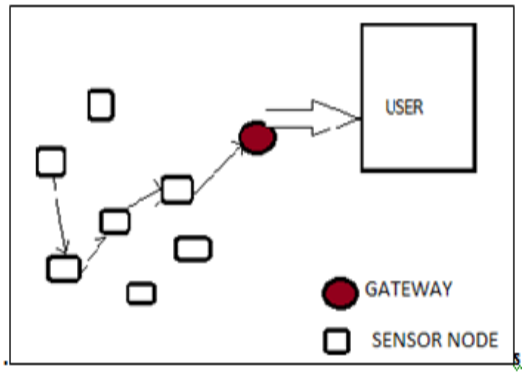

Fig. 1:

A. WSNRequirements

Depending on the applications WSNs have different types of requirements. Mainly it is important that all sensor nodes work properlyanditisgoodiftheirlifetimeisidenticalformos tofthe sensor nodes. Why because WSNs are

usually battery powered applications,sothatthelifetimeofaWSNisimportant.Therefore the algorithms which run on them must be optimized andtested. These algorithms run on tiny Micro controlling devices (MCU) whicharelimitedinprocessingandstoragespace.Since thegoal of a WSN is to make that all sensor nodes workproperly.

B. Problems andIssues

A main issue with all wireless devices is their battery power consumption; the more data are being transmitted, the larger the battery consumption is. One way to attack this problem is to reducethebittransmission.TheBittransmissioncanbereducedbyaggregatingsensordata.Thisapproachtotheproblemcannot be applied in all WSNs, but it can be applied where theaverage, variance,maxormintemperature,humidityorsomeothersensing property is of vital importance for theWSN.Therearenumberofprivacyschemessuchas[1,9,1115]havebeenproposedforWSNs.Theexistedprivacyschemesespecially[1]mainlyfocusedonthealgorithmsrelatedtoidentity,routeandlocation of the sensor nodes. Although the privacy schemesof[1]discussedaboutthedataprivacyscheme butnotsuggestedany algorithm for providing efficient data privacy forWSNs.SonowinthisIamproposinganalgorithmfor providingefficient data privacy for WSNs. My contribution lies in the following: RSA algorithm for encryption and random numbergeneration.

II. RELATED WORK

A. Privacy Schemes

There are number of privacy schemes [1, 9-15] are proposed for
WSNs. They are:

- Phantom routing scheme and Phantom single-path routing scheme for WSNs, which helps to prevent the location of a source from theattacker.
- Simple Anonymity Scheme (SAS) and Cryptographic Anonymity Scheme (CAS) for establishing anonymity in clusteredWSNs.
- GreedyRandomWalk(GROW)schemetoprotectthelocationof the source node.

B. Adversary Model

We assumed that an adversary can perform passive attacks why because such attacks help to conceal the adversary's presencein the network.
If the adversary is also capable of performing active attacks like fabrication and packet drop attacks. We also assumed that the adversary is both device-rich and resource-rich [4].
These characteristics are defined below.

- CyclicEntrapmentMethod(CEM)tominimizethechanceof • an adversary in finding out the location of the sourcenode.

Butnoneoftheaboveschemesprovidingfullnetworklevelprivacy
as collectively or separately. The first solution for providing full network level privacy [1] for WirelessSensor Networks:

- Identity, Route and Location (IRL) privacyalgorithm.
- Reliable Identity, Route and Location (r-IRL)privacyalgorithm.
- A data privacymechanism.

Device-rich:theadversaryisfullyequippedwithdevices.Forexampledeviceslikeantennaandspectrumanalyzer.Sothat the adversary can measure the angle of arrival of thepacket and received signalstrength.
Resource-rich:theadversaryhas no resource constraint in computationpower,memoryorenergy.Itisalsoassumedthat theadversary has basic domain knowledge like the rangeof identitiesassignedtothesensornodes,thepublickeyofthe basestationandinformationaboutthecipheralgorithmsuse
The data privacy mechanism that is mentioned in the above [1]is the source for this paper.

III. NETWORK AND ADVERSARYMODEL

A. Network Model

- Wireless Sensor Networks (WSN) are composed of large number of small sensor nodes which consists of limited resources and densely deployed in an environment.
- Whenever the users require information about any event related to some object(s), they send a query to the sensor network via the basestation.
- Thenthebasestationpropagatesthatquerytotheentirenetwork or to a specific region of the network.
- Then sensor nodes send back required information related to that query to the basestation.
- AtypicalwirelesssensornetworkscenarioisshowninFigure

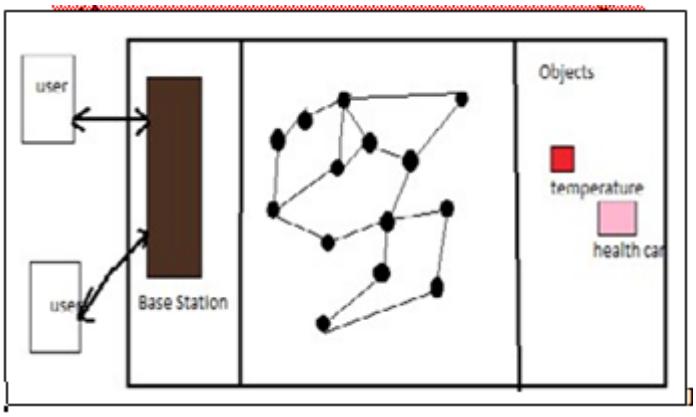

Fig. 2: Wireless Network

2. inthenetwork.However,adversaryhasnoknowledgewhich identity is physically associated with whichnode.

IV. PROPOSED SCHEME

As mentioned in the introduction, encryption plays a major role in all today's communication systems, especially in military or WSNs applications. The proposed scheme is for providing data privacy for WSNs i.e. encryption of data using some algorithm. InthispaperRSAalgorithmwasusedtoprovideencryption.For better performance random number generation is also used in that algorithm.

A. Data PrivacyMechanism

Thepayloadcontainstheidentityofthesourcenode(IDs)andtheactualdata(d).Identityisencryptedwiththepublickey(ke+bs)of thebasestationanddataisencryptedwiththesecretkey(kp,bs) shared between the sender node and the BS. Both are appended with the payload as shownbelow:payload = [En(IDs, ke+bs),En(d, kp,bs)]

If we assume that the adversary knows the range of identities assigned to the sensor nodes, public key of the base station and information about cipher algorithm used in the network, an adversary can then successfully obtain the identity of the source byperformingsimplebrute-forcesearchattackbycomparingthe pattern of encrypted identity with a known range of identities. Thereforeinordertoprovideprotectionagainstbrute-forcesearchattack,weappendarandomnumber(Rn)(equivalenttothesizeofidentity)withtheidentityofanodeandthenperformencryption. Now the payloadis:payload = [En(IDs||Rn, ke+bs),En(d, kp,bs)]

- Encryptionofdata:Encryptingdataisawayofencapsulatingtheinformationandprotectingitfromtheoutsideworld,inthat sensethatnobodyshouldbeabletoknowwhatinformationis
- Intheabovefigurethelinksbetweenthesensornodes,basestation and end user are bidirectional.
- Alsosensornodeskeepspacketsinitscacheuntilth esenderreceives an Acknowledgment (ACK).It means they use IEEE •802.11 standard link layer protocol.
- Whenever a receiver node successfully receives thepacketit will send back an ACK packet to the sender.
- If the sender node does not receive an ACK packet during pre defined threshold time, then the sendernodewillretransmitthatpacket.insidethepacketbesidethedevice/personwhoshouldreceive it. The author goal was to achieve an end-to-endencryption between the nodes and thesink.

End-to-end encryption: In end-to-end encryption no node should be capable of knowing or being able to extract the informationfromthereceivedpacketsbesidethesink.Using this approach it is possible to guarantee that it will be more difficultforaneavesdroppertogainaccesstothedata.Another way of addressing the encryption problem would be to use a global encryption key or only keys between neighbouring nodes,butinthatcasetheend-to-endencryptionislost.For thefirstapproach,havingoneglobalkey,aneavesdropper

couldgainaccesstoallinformationbyjusthackingonenode and determining the global key.

B. Suggested EncryptionAlgorithm

1. KeyGeneration

In every next level of the k-ary tree, the transmission bit-length for the node in that level grows exponentially. In other words, in a 3-ary WSN tree of height 3,nodes in the third level transmit their encrypted samples, nodesinthesecond level transmittheir own read sample and the other three sample values which they received from their predecessors, without the header, footerandGeneratetwolargerandomprimes,aandb,of

approximately equal size suchthattheir product p = ab is of the required bit length, e.g. 1024 bits.
Compute p = ab and (phi) φ = (a-1) (b-1).delimiter.

VII. CONCLUSION AND FUTUREWORK

This paper mainly concentrates on providing data privacy for

(iii) Choose an integer d, 1 <d < phi, such that gcd(d, phi) =1.
(iv) Compute the secret exponent e, 1 < e < phi, such that de ≡ 1 (mod phi).

WSNs,the idea which was taken from the existing system [1]. Sotheproposed systemis providing privacyforWSNsbyusing the RSA algorithm. By using the RSA providing encryptionand

Thepublickeyis(p,d)andtheprivatekey(e,a,b).Keepal l
the values e, a, b and phi secret.
random number generation which supports efficient data privacy for WSNs.This paper concludes that it provides efficient data

(v) [Weprefersometimestowritetheprivatekeyas(p, e)because you need the value of p when usinge.]
- p is known as the modulus.
- disknownasthepublicexponentorencryptionex ponentor just the exponent.e is known as the secret exponent or decryptionexponent.

2. Encryption
- Sender A does thefollowing:-
- Obtains the recipient B's public key (p, d).
- Represents the plaintext message as a positive integer m,1

< m < p .
- Computes the ciphertext c = md mod p.
- Sends the ciphertext c toB.

3. Decryption

Recipient B does the following:-
- Uses his private key (p, e) to compute m = ce modp.
- Extracts the plaintext from the message representative m.

4. Digital Signing

Sender A does the following:-
- Creates a message digest of the information to besent.
- Represents this digest as an integer m between 1 and p-1.
- Usesherprivatekey(p,e)tocomputethesignatures =

me mod p.
- Sends this signature s to the recipient,B.

5. Signatureverification

Recipient B does the following:-
- UsessenderA'spublickey(p,d)tocomputeinteger v=

sd mod p.
- Extracts the message digest from thisinteger.
- Independentlycomputesthemessagedigestofthein formation that has beensigned.
- If both message digests are identical, the signature isvalid.

VI. RESULTS AND ANALYSIS

A. Theoretical Analysis

The no aggregation method just forwards the packets received towardsthesink.Inthiscase, all packets
areencrypted(itcouldbeanyencryptionalgorithmsche measwellasahomomorphic,but the property of aggregating data is not used) and beside thesink none of the nodes knows what is inside the packet. This method offers the best end-to-end privacy option, however the waste of bandwidth is obvious.privacy for WSNs.
The future work can be done in the way of aggregating the data. Aggregating data is a way of compressing the transmitted packet, in a sense that the packet is comprised of onlynecessary information [4].

REFERENCES

[1]. Riaz Ahmed Shaikh,HassanJameel,Brian J.d'Auriol, Heejo Lee, Sungyoung Lee, Young-Jae Song," Achieving Network Level Privacy in Wireless SensorNetworks".
[2]. "Federal Hydrometeoro logical Institute", [Online] Available: http:// www. fhmzbih.gov.ba/ engleski/index.php,
[3]. "Predator drones hacked in Iraq operations", [Online] Available: http://www.cnet.com, 2009-12-24,2009.
[4]. Gene Tsudnik Claude Castellucia,Einar Mykletun, "Efficient aggregation of encrypted data in wireless sensor networks".
[5]. Hans Delfs, Helmut Knebl,"Introduction to Cryptography: Principles and Applications", Springer,2002.
[6]. HolgerKarl,AndreasWillig,"ProtocolsandArc hitecturesfor Wireless Sensor Networks.", John Wiley & Sons,2005.
[7]. StevenSmith,"DigitalSignalProcessing:APra cticalGuide for Engineers and Scientists", Newnes,2002.
[8]. C. Tharini, P. Vanaja Ranjan,"Design of modified adaptive huffman data compression algorithm for wireless sensor network", Journal of Computer Science

5,2009.

[9]. Xi,Y.;Schwiebert,L.;Shi,W.,"PreservingSourceLocation Privacy in Monitoring-Based Wireless Sensor Networks", In Proceedings of Parallel and Distributed Processing Symposium (IPDPS 2006), Rhodes Island, Greece,2006.

[10]. Habitat monitoring on Great Duck Island (Maine, USA), 2002. [Online] Available: http://ucberkeley.citrisuc.org/research/projects/greatduckisland(accessedon21August, 2009).

[11]. Ozturk,C.;Zhang,Y.;Trappe,W.,"Source-LocationPrivacy in Energy-Constrained Sensor Network Routing", In Proceedings of the 2nd ACM workshop on Security of Ad hocandSensorNetworks,Washington,DC,WA,USA,2004; pp. 88–93.

[12]. Kamat, P.; Zhang, Y.; Trappe, W.; Ozturk, C.,"Enhancing Source-Location Privacy in Sensor Network Routing", In Proceedings of the 25th IEEE International conference on DistributedComputingSystems,Columbus,OH,USA,2005; pp. 599–608.

Manmath Nath Das“ WSN: An Effective Data Privacy Arrangement ” *International Journal of Engineering Research and Applications (IJERA*), vol.6(9), 2016, pp 99-103.