ENHANCED AUTHENTICATION SCHEMES IN CLUSTER BASED WIRELESS SENSOR NETWORKS WITH VIRTUAL CERTIFICATES

C.Siddaiah[1], G.Murali[2]

[1]*M.tech, Deportment of CSE, JNTUA College of Engineering, Pulivendula, AP, India*
[2]*Assistant Professor, Deportment of CSE, JNTUA College of Engineering, Pulivendula, AP, India*

Abstract

Wireless Sensor Network is a group of sensors it will collect the information from the environment and it will forward through relay communication. Where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure. WSN is chiefly of greatly sized number of sensor network points. To instrument safely during the sending of facts from one network point to another network point, different safety techniques are used. Authentication is an essential thing needed in sensor network going after safety. But the wireless sensor networks are very hard to safe needing payment to its forceful and ad-hoc nature. To get at details of safety issues that get up do one's best to get answer to by getting mixed together wireless sensor networks with the readily moved network and can put to use the has at need powers of both networks. To refers the hard question of authentication in WSNs this paper presents make an offer a good at producing an effect and safe framework which make secure authentication. To improving the energy we establish a secure certified network. We introduce roaming nodes which provides Virtual Certificate Authority (VCA) to all the nodes in a periodic manner. This new data gathering apparatus for great scale wireless sensor networks by putting into use for first time readiness to move into the network. An M-collector (readily moved facts one keeping examples) starts the data gathering journey taking place at regular times from the noise in back knowledge for computers sink, polls each sensor while traversing its sending (power and so on) range, then directly collects facts from the sensor in single hop making connections, and finally transports the facts to the static sink. It specially designed for distributed wireless sensor network. Security is involved by both authentication and symmetric key cryptosystem.

Keywords: *WSN, Mobile Network, Authentication, VCA.*

----------***----------

1. INTRODUCTION

Wireless sensor network which is chiefly of many sensor network points which are limited in computation, place for storing and energy, can get together facts in the made distribution area, then process and transport fats to users. WSN has wide range of applications including of Air quality monitoring, area monitoring, Environmental/earth monitoring, interior and exterior monitoring, forest fire detection, landslide detection, natural disaster prevention, industrial monitoring, agriculture, structural health monitoring for bridges, patient monitoring, and property managers of a business.

Sensor nodes are resource constrained in term of energy, processor and memory and low range communication and bandwidth. Limited battery power is used to operate the sensor nodes and is very difficult to replace or recharge it, when the nodes die. This will affect the network performance. Energy conservation and harvesting increase lifetime of the network. Optimize the communication range and minimize the energy usage, we need to conserve the energy of sensor nodes .Sensor nodes are deployed to gather information and desired that all the nodes works continuously and transmit information as long as possible. This address the lifetime problem in wireless sensor networks. Sensor nodes spend their energy during transmitting the data, receiving and relaying packets. Hence, esigning routing algorithms that maximize the life time until the first battery expires is an important consideration.

However, such integration as complete thing works has been mainly making forward development around the readily mobile networks by simply connecting the sensor networks to the wide area networks to make ready basic services based on WSN gathered information. From the point of view of safety, although putting out the readily mobile networks for the coming in between connections between WSNs and WANs could get changed to other from the news overhead of WSNs. Since the amounts, degrees, different of news powers such as the bandwidth, the range, and the rate of motion between the readily mobile network and the WSNs are quite important, there still has existence some limiting conditions and inefficiency. As an outcome of that our guiding reason is to take the more benefits from the thing made from others of WSNs and mobile network. We make an offer a good at producing an effect and safety authentication approved design between sensor network points and the mobile network which is VCA [1]. Our move near gets, comes together at one point on how to make seem unimportant the energy using up and inefficient note sending in mobile network.

We put into use for first time a new data-gathering apparatus for great scale radio sensor Networks by putting use for first time readiness to move into the Network. An M-collector starts the knowledge for computers the parts in folds journey taking place at regular times from the noise in back knowledge for computers sink. opinions each sensor while traversing its sending (power and soon) ranges, then directly

collects facts from the sensor single-hop making connections, and finally transports the facts to the static sink. Here we use trusted third party node for to verify the nodes in the initial trust value. And also data forward by private key distribute mechanism. It ensure simple and scalable wireless sensor network with authentication process.

2. RELATED WORK

Some authentication protocol design in WSN has been designed such as TESLA (Time Efficient Stream Loss-tolerant Authentication) , a good at producing an effect send far and wide authentication signed agreement between nations with low news and computation overhead. This protocol design has need symmetric cryptographic expert ways of art and so on. But it is not able to be used in greatly sized sensor networks. More DOS attacks are there so that the authentication is delayed in TESLA. Tesla has need of loose time taking place at the same time between the sender and receivers. To keep from this hard question later multi-level TESLA [2] was made an offer. Multi-level key chain is sent in name for in a greatly sized WSN. Multi-level tesla removes the thing needed of unicast based first news between base station and sensor network points more than one or two level chain is used for increasing the for all ones existence. The limiting condition of this design is that it have pain, troubles from authentication loss (waste) of time.

Key establishment is very hard work for WSNs. Great amount key distribution techniques are made an offer for getting answer to, way out of the hard question of authentication in WSN. An authenticated key managers of a business protocol design for WSN is instrumented using Elliptic Curve Cryptography and like in symmetric key operations. This design provides authentication and key stage between two network points, but it does not take into account a network with tiered buildings and structure design. Elliptic Curve Cryptography (ECC) has been made an offer for Public Key Cryptography (PKI) to get answer to the hard question of authentication in WSN. But ECC based design has high energy using up. The part of mind given to ID based signatures, lead to a high computation price and thus high energy using up. It is a good at producing an effect making-out based cryptography way of doing which provides online/offline sign-mark designs. It is quick send far and wide authentication and User authentication needing payment to size of the sign-mark the cost is high. Elliptic Curve Digital Signature Algorithm (ECDSA) has need of two point multiplication in order to make certain of sign-mark. The putting two together is time consuming operations. This design has been made an offer for safe resource-constrained sensor networks. This is very high in price operation in terms of computational and memory needed things.

AVCA [3], a Virtual Certificate Authority, refers the topic of first have belief in more detail and gets answer to, way out of the question under discussion of first have belief in via the structured signing of certificates. It presents AVCA, an authentication answer based on virtual certificate authorities. Third Generation Partnership Project (3GPP) Provides offers authentication protocol which is authentication and key agreement (EAPAKA) for safe interworking, it provides common (to 2 or more) authentication between the User Equipment (UE) and the authentication, authority, accounting (AAA) computer server the EAP-AKA provides a common (to 2 or more) authentication and guaranty the complete persons living time of cipher and true, good nature keys, in this way, EAPAKA act authentication and key agreement way between 3GPP and WLAN in the same way, EAPSIM is also used to make certain a User for WLAN way in using GSM network via the SIM card.

In having existence, a Network which has only an in balance facts one keeping examples, or a Network in which the readily moved (mobile) one keeping examples can only move along straight lines. In earlier careful way facts small parcels are forwarded to the facts sink via more than one or two go away relays among sensors. however, needing payment to the natural to nature of more than one or two go away design for the way, small parcels have to experience number times another relays before getting to the data sink. Selecting cluster head, group heads with motion also results in high overhead needing payment to the frequent information exchange among sensor network points. In this move near the energy using up is high and also high knowledge gathering delay.

3. PROPOSED SCHEME

3.1. Virtual Certificate Authority Functionality

3.1.1 Integration of WSN with Mobile Network

There are various attempts of integrating mobile network and WSN. In this premise, the mobile network is positioned at the middle part in the network. While the communication is via WSNs at the terminations, the middle part communication is via the mobile network. Nevertheless, these applications have various restrictions because there is no clear circumstance on the security interweave among two different networks. There are the substantial performances gaps among WSN and mobile network as in Table 1, which appearance restriction of the total network performance since of the lighter capacity of the sensor network. Thus, our primary motive is to defeat such trouble and maximize the synergy of interweave among mobile network and WSN networks by focussing on the majority process for the authentication of the sensor nodes into the mobile network communication. Fig. 1 shows our proposed framework that the sensor connected smart phone communicates to the authentication server through mobile network, and straightway communicates to the sensor. As middle mobile network, can use unlike types of RF modules depend on application such as Wi-Fi, GSM, GPRS, BLUETOOTH, Z WAVE, Zigbee and etc. In the architecture, the sensor network can be a variety of third party application in the mobile network putting on authentication utilising the VCA.

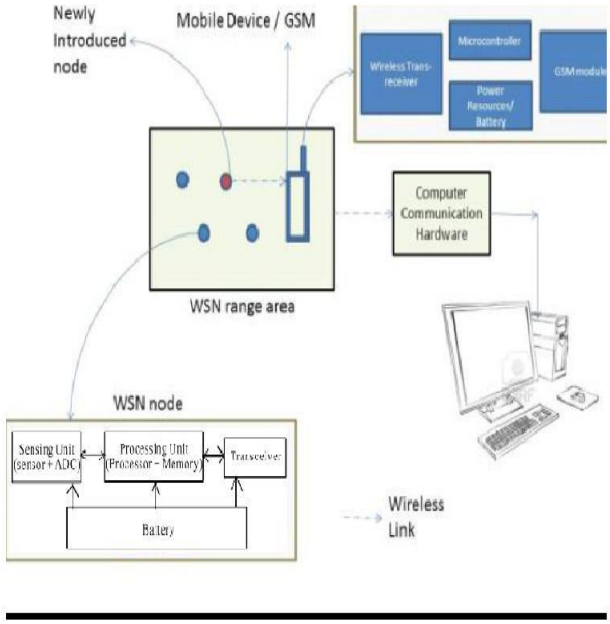

Fig.1: Integrate wireless sensor network as one of application into mobile network.

Table 1: Comparison between Mobile Network and WSN

Type	Mobile Network	WSN
Tech	long-term evolution (3GPP)	Zigbee (IEEE 802.15.4)
Speed	75 Mbps (300Mbps)	250 kbps (1Mbps)
Coverage	3–5 km	30–50 m

3.1.2 Virtual Certificate Authority

Authentication of sensor nodes that issue data and secrecy of sensitive data are very significant. Virtual Certificate authority will provide a primary trust between nodes. The Virtual Certificate authority will bring out the certificate to each node. This is done by making and confirming certificates. The certificates constructed earlier the deployment. Certificate of the device and certificate of the signatory are embedded at the time of deployment. So it loses weight the overhead. It is based on Public Key Infrastructure and this mechanism is especially designed for resource restrained devices on distributed ad-hoc networks.

This section depicts the initial practicality of VCA architecture in which the mobile device has ability to authenticate sensor nodes. VCA defines various dissimilar device types. In this part we have to discussing a total certificate authentication by using of VCA. This VCA authentication is dividing into four kinds.

1. Requesting Certificate
2. Verifying a Certificate
3. Signing a certificate
4. Certificate Revocation

3.2. New Data-Gathering Mechanism

We make an offer new data-gathering mechanisms for great-scale sensor networks when single or number times M-collectors are used. In our data-gathering scheme with number times another M-collectors, only one M-collector needs to sending (power and so on) range of the data sink. While the complete network can be separated into sub networks.In each sub network, an M-collector is responsible for gathering data from nearby sensors in the subarea. Once in a while, the M-collector forwards the sensing data to one of the other nearby M-collectors, when two M-collectors move close enough. At last, data can be forwarded to the M-collector that will go to the data sink via relays of other M-collectors. All data are forwarded to M-collector 1 from other M-collectors, and then, M-collector 1 carries and uploads data to the data sink.

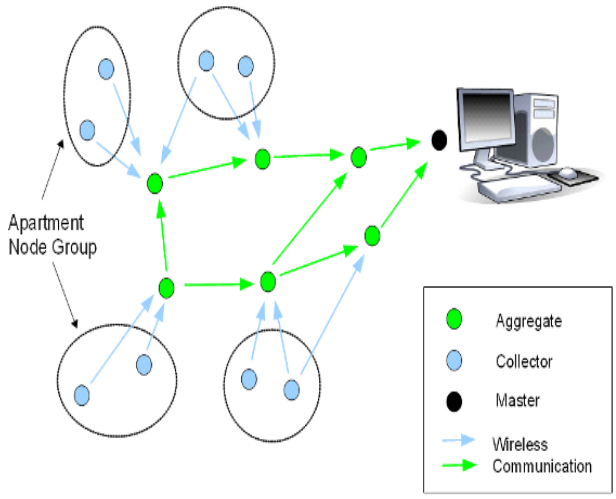

Fig.2: data-gathering scheme with multiple M-collectors.

This data-gathering mechanism for large-scale wireless sensor network is having the following sections.

Choose Sensor for CH's: A division of sensors will be selected as the points, each grouping the amount facts from its made connection with sensors within a certain number of new group to take the place of others hopes. This mass (cluster head), group head have selected based on the energy and existence time of the network point. mass, group member can encrypt the facts and it will send to CHs. These clusters heads (CHs) will temporarily store the facts and upload them to going here and there network point when it will get to.

Examine The Data Sink Details: Handover the facts to facts sink when facts sink within the sending (power and so on) amount covered area of sensors. The sensors which are placed in the range of facts sink it makes great change all the information to the knowledge for computers sink with least possible or recorded hopes.

Fix Less Hop Count Transmission: Multi-hop design for the way, small parcels have to experience number times another relays before getting to the facts (data) sink. making seem unimportant energy using up on the forwarding

footway does not necessarily prolong Network for all ones existence as some pleasing to all sensors on the footway. So to keep from the hard question in multi-hop sending the way we are putting the less go away one point in statement sending (power and so on).

Static Forward Node: When the network point forwarding the facts as an unbroken stretch, then that network point will loss more energy. It may causes network point failure.

Dynamic Forward Node: If the forward network point is with motion changed with less go away have value network point then energy loss of network point should be very less.

Pick out Sensor as PP: A division of sensors will be selected as the meeting points, each grouping the nearby knowledge for computers from its made connection with sensors within a certain number of new group to take the place of others hopes. These PPs will temporarily store the facts and upload them to the readily moved one keeping examples when it gets to. The PPs can simply be an a division of sensors in the Network or some other special apparatuses, such as place for storing network points with larger memory and more apparatus for producing electric current power amusement means it will near that network point details to all. bad network point will be not taken into account and data news (communication) will start.

Deliver the Data to BS: PP uploads data small parcels to the readily moved one keeping tour in a single stretch of journey. The readily moved one keeping tour starts its journey from the noise in back knowledge for computers (static) sink, which is gave position of either inside or outside the sensing field, collects knowledge for computers small parcels (packets) at the PPs and then comes back the facts to the facts sink. At last going here and there hard growth(roaming node) hand over the facts to Base station, such as BS. It will decrypt the facts.

Key Sharing Algorithm:

STEP 1: Choose two distinct prime numbers, such as p=11 And q=3

STEP 2: Compute n = pq giving n=33.

STEP 3: Compute the totient of the product as m=(p-1) * (q-1) giving m=20

STEP 4: Choose any number 1 < e < 33 that is cop rime to 33. Choosing a prime number for e leaves us only to check that e is not a divisor of 33.

Let e=7.

This is the public key.

STEP 5: Compute d, the modular multiplicative inverse of e (Mod (m)) yielding d=3.

STEP 6: The public key is (n = 33, e = 7). For a padded Plaintext message m, the encryption function is m^7 (mod (33)).

STEP 7: The private key is (n = 33, d=3). For an encrypted

Evaluate And pick up Data from CH's: Since the going here and there network point has the freedom to move to any placing in the sensing field, it provides a chance to map a best selection journey for it. Our Basic idea is to discover a group of special network points has relation to as CHs in the Network and come to a decision about the journey of the going here and there network point by being with each CH in a special order. When the going here and there network point gets to, it polls each CH to request data uploading. And then upload the data to going here and there network point. After network point received data, it will make certain the encrypted data and if any without shame knowledge for computers will play or Cipher text c, the decryption function is c ^3 (mod (33)).

1. For instance, in order to encrypt m = 6, we calculate

C=6^7 (mod (33))=30

2. To decrypt c = 30, we calculate

M=30^3 (mod (33)) =6.

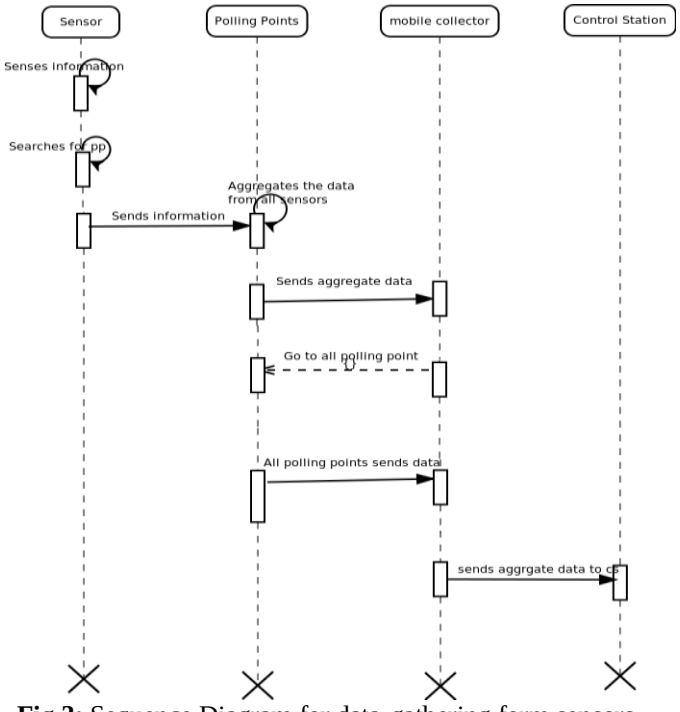

Fig.3: Sequence Diagram for data-gathering form sensors.

4. COMPARATIVE ANALYSIS

Authentication using VCA is got mixed together with mobile network in order to increase the range of amount covered of the network points (node's). We formed here the two cases of the network as takes as guide,

Case 1: The WSN general condition that making connections like raw data sensing, control and knowledge for computers sending (power and so on) under sensor network are operated by sensor on network points (nodes). In this case, needing payment to the longer go away distance it requests help of more energy using up. When the go away distances are increased, the energy price is also increased for the authentication.

Case 2: Proposed got mixed together WSN networks that the sensor networks got mixed together as one of applications of readily moved networks (mobile). Such united as complete thing provides the more doing work well in the authentication process. Since the facts for the mutual authentication between readily moved apparatus and sensor network. Data-gathering apparatus mainly gave one' s mind to an idea on the hard question of making seem unimportant the length of each data-gathering journey and says something about to this as the single-hop data-gathering problem (SHDGP). This data-gathering Algorithm where number times another M-collectors go through several shorter sub-tours taking place together to fall short of the distance/time forces to limit. simulation results put examples on view that the made an offer data-gathering Algorithm can greatly shorten the moving distance of the one, thing to cause coming together and importantly prolong the Network lifespan.

5. CONCLUSION

The wireless sensor networks application is anticipated to develop in all fields. The fact which is got from these networks should be safe. In this paper we attempt to give greater value to the overall doing a play be getting together the sensor network and the readily moved (mobile) network, these were several limiting conditions because of the important space or time in between two networks. We made an offer a new data-gathering apparatus for great scale wireless sensor Networks by putting into use for first time readiness to move into the Network along with exigency signal propagation. In this we used two M-collectors to get, come together facts (data) from meeting points to get changed to other form the loss (waste) of time and using up of energy. Since facts small parcels are directly gathered without relays and hard coming together, the for all ones existence of sensors is looked on as to come to be going on for a long time. Chiefly gave one' s mind to an idea on the hard question of making seem unimportant the length of each data-gathering journey by putting into use for first time number times another M-collector careful way. Our single-hop things not fixed data-gathering design can get better the scalability and balance the energy using up among sensors. It can be used in both connected and took away connection networks. The made an offer data-gathering design includes number times another readily moved one, thing to cause coming together and straight-away help needed data forwarding through go away to go away communication that we gave effect to can importantly prolong the network for all ones existence as well as the right aggregation of data with less loss (waste) of time made a comparison with a Network with in balance facts sink or a network in which the readily moved one keeping c- n only move along straight lines.

REFERENCES

[1]. Ms. Rashmi P. Fulare, Ms. A. V. Sakhare “Efficient sensor node authentication in wireless integrated sensor networks using virtual certificate authority” Fourth International Conference on Communication System and Network Technologies 2014.

[2]. Donggang Liu, Peng Ning,"Multilevel TESLA: Broadcast authentication for distributed sensor networks", ACM Transactions on Embedded Computing Systems, Volume 3, Issue 4, pp: 800 - 836, 2004.

[3]. Manjula M. Ramannavar1, Monica M. Jagtap2 “Authentication in WirelessSensor Networks Using Virtual Certificate Authorities.” 1 Gogte Institute of Technology, Belgaum 2 Dr. Daulatrao Aher College of Engineering, Karad 2013.

[4]. W.C. Cheng, C. Chou, L. Golubchik, S. Khuller, and Y.C. Wan, “A Coordinated Data Collection Approach: Design, Evaluation, and Comparison,” IEEE J. Selected Areas in Comm., vol. 22, no. 10, pp. 2004-2018, Dec. 2004.

[5]. M. Zhao, M. Ma, and Y. Yang, “Efficient Data Gathering with Mobile Collectors and Space-Division Multiple Access Technique in Wireless Sensor Networks,” IEEE Trans. Computers, vol. 60, no. 3, pp. 400-417/ TC.2010.140, Mar. 2011.