International Journal of Scientific Research and Engineering Development-– Volume3 Issue 1, Jan-Feb 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Design & Development Of An Effective Key Management in Dynamic WSNs Using Certificate Less- Effective Key Management Protocol For Secure Communications Characterized By Node Mobility

Kusha K.R.
Research Scholar(1SI17PEA08), VTU, Belgaum, and
Assistant Professor, Dept. of Computer Science & Engg.(CSE)
Reva University, Bangalore, Karnataka, India
Email : kusha.karur@gmail.comMobile : 9738462560

Dr. Purohit Shrinivasacharya
Associate Professor, Dept. of Information Science & Engg.
Siddaganga Institute of Technnology, Tumkur, Karnataka, India
Email : purohitsn@gmail.comMobile : 9448176001

***Abstract*—In this paper, the design & development of an effective key management in dynamic WSNs using certificate less-effective key management protocol (CL-EKM) for secure communications characterized by node mobility is being presented. It is a well-known fact that a wireless sensor network (briefly abbreviated as WSN) is a dedicated sensor monitoring system for recording the state or condition of a network, which consists of a number of parameters called as nodes (source & sink), the recorded data being maintained at a central location. As there are 2 types of WSNs,viz., static WSN&mobile WSN,each one has got advantage over the others. As the topic of concern of our work is related tom WSNs,the same is being presented in this context. The simulations are performed in NS-2 platform and the results shows the effectiveness of the methodology developed.**

***Keywords*— WSN, Authentication, Sensor, Node, Key Distribution, Network, Key, Message Authentication Code Protocol, Security, Routing, Management, Sink, Cryptography, Source, Energy, Attack.**

I. INTRODUCTION TO WSN & ITSTYPES

A WSN is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates gateway that provides wireless connectivity back to the wired world and distributed nodes. The wireless protocol could be selected depends on the application requirements. Some of the available standards include 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz[3][4].

These are similar to the wireless adhoc networks in the sense that they rely on wireless connectivity and spontaneous formation of networks so that sensor data can be transported wirelessly. WSNs are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure,etc. and to cooperatively pass their data through the network to a main locations. The more modern networks are bi-directional, also enabling control of sensor activity. A general topology of a WSN is shown in the Fig. 1, which also shows the sensor node & the sink node [3].

There are two types of WSNs, one is a static WSN & the other is a dynamic or mobile WSN. Static Wireless Sensor Networks. A static wirelesses so network(SWSN) cansimply be defined as a wireless sensor network (WSN) in which the sensor nodes are static in nature. A mobile wireless sensor network (MWSN) can simply be defined as a wireless sensor network (WSN) in which the sensor nodes are mobile in nature (bidirectional movement). MWSNs are a smaller, emerging field of research in contrast to their well-established predecessor. MWSNs are much more versatile than static sensor networks as they can be deployed in any scenario and cope with rapid topology changes. As the topic of concernin *m*-WSNs,the block diagram of the same is shown in the Fig. 2. The research work taken up in this paper is related to the mobile dynamic wireless sensor networks wherein the security keying plays a very importantrole.

The paper is organized as follows. A brief review of the WSNs & its types was presented in the section I. The static & dynamic Key Management process is presented in sections II followed by the proposed research methodology in section III along with the hardware & software tools needed for the simulation purposes. An exhaustive review of the related literature w.r.t. the work done by various authors is presentedin section IV. The section V presents the review of the proposed related works, which is followed by the existing WSN system models in section VI. Then, the developed model is presented in section VII. The NS-2 simulations are presented in section VIII followed by the advantages of the developed methodology in section IX. The conclusions are presented in section X followed by the references.

 ©IJSRED:All Rights are Reserved

II. STATIC & DYNAMIC KEY MANAGEMENTSCHEMES

The static schemes assume that once administrative keys are pre-deployed in the nodes, they will not be changed. Administrative keys are generated prior to deployment, assigned to nodes either randomly or based on some deployment information, and then distributed to nodes. Key management schemes in sensor networks can be classified broadly into dynamic or static solutions based on whether rekeying (update) of administrative keys is enabled post network deployment. The objective of key management is to dynamically establish and maintain secure channels among communicating nodes. Numerous key Management schemes have been proposed for sensor networks. Most existing schemes build on the seminal random key pre-distribution scheme introduced by Eschenauer and Gligor [14][24]

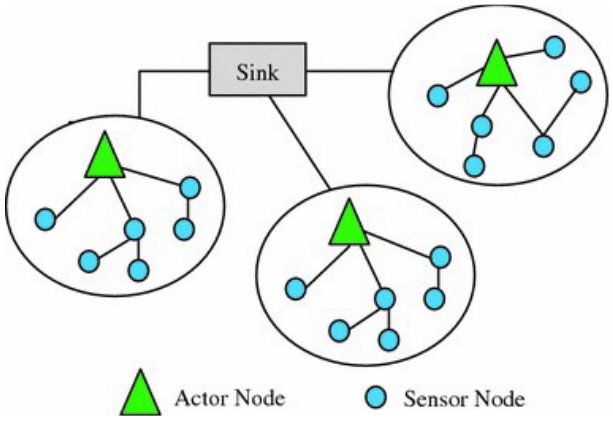

Fig. 1 : A WSN showing the sensor node & the sink node.

A general topology of a mobile WSN is shown in the Fig. 4.

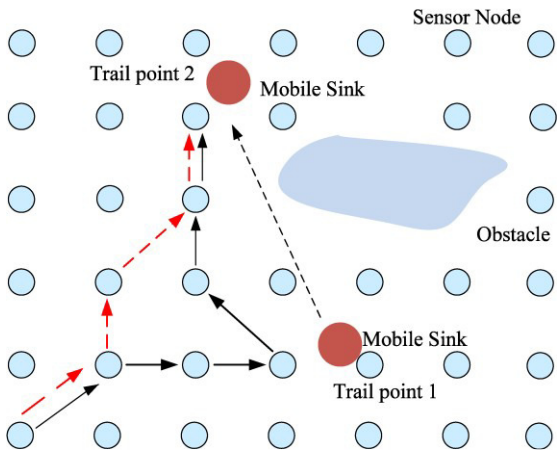

Fig. 2 : General structure of a *m*-WSN

III. PROPOSED RESEARCHMETHODOLOGY

In this section, the proposed methodology for development of enhanced secure key management framework in dynamic mobile wireless sensor networks is being presented with the contributory work that is already being implemented and presented in this context along with the simulation results.

Due to the dynamic changes in the network, the security has to be given more importance in order to protect the data as well as to maximize the lifetime of the network. While providing the security for the network, the key management plays a major role in it. Using a single network wide key gives up the entire network if the single key has been compromised. By using pairwise keys, it improves the security as well as the lifetime of the network but lacks in scalability due to the memory constraint.

Thus, changing the key dynamically provides more security and also improves the lifetime of the network. The parameters that are used for dynamic key generation should be chosen carefully in such a way that the intruders should not predict them. Since the keys are dynamically changed, it increases the communication overhead in order to share it with the neighbouring nodes or the destination. This overhead can be reduced by the design of key management technique or the protocol.

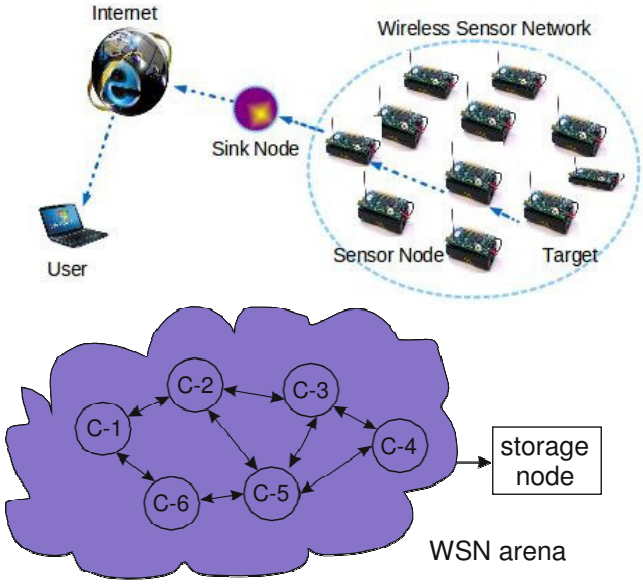

Fig. 3 : The system architecture with the group of cluster heads
User – Source node, Target – Destination node

It has to be noted in this context that the key deployment is similar to the OTP generation in the mobiles for secure transactions. Since many applications require the support of mobility, the dynamic & efficient clustering algorithm has to be designed w/o compromising the security of the n/w. The network architecture also plays an important role in providing security and doing complex tasks such as key management, secureclustering,secureroutingetc.Deployingmorenumberof heterogeneous nodes improves the performance of the network but it is not cost effective. So the heterogeneous nodes have to be deployed optimistically in the field. The above mentioned approach of secure keying development is well explained pictorially in a very highly abstracted manner in the Fig. nos. 3 & 4 respectively. The proposed methodology mentioned in the previousparagraphsisusedfordevelopingthesecurityprotocol in the WSNs in thispaper.

 ©IJSRED:All Rights are Reserved

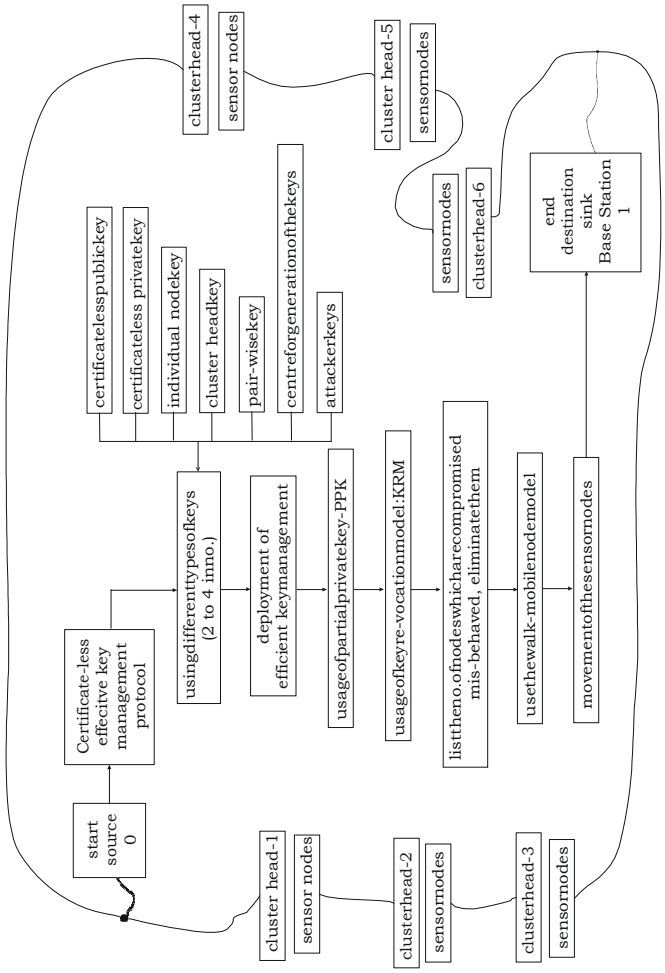

Fig. 4 : Data flow diagram approach used in the development of the proposed block-diagram for the data transmission

A. *Software toolused*

The software tool that is used for the research work is the NetworkSimulation(Ver.2)&varioustoolboxesalongwithit. Ubuntu is the environment that is chosen for the simulation. Coding (programs) are developed as **.**tcl scripts files, the developed codes are run after giving the necessary datas as the input and after the simulation is over, the results are observed from which we can draw sufficient conclusions and inferences. Other tools such as C++ language, Matlab & LabVIEW could alsobeusedforthecoding&algorithmdevelopment,butinour work,NS-2isbeingusedasitsurpassesallthedisadvantagesof Matlab & LabVIEW and provides a good platform the networkingengineers.

B. *Hardware/Software System Specifications:*

Thehardware&softwaresystemspecificationsthatareusedfor the simulation purposes are mentioned as underherewith.

Hardware Specification -

Mainprocessor	:	Dual Core
Hard diskcapacity	:	1 TB (min)
Cache memory	:	4GB
RAM	:	8 GB
Monitor	:	Flat screenLCD
Mouse	:	Logitech3-button

Software Specification -

Operatingsystem	: Linux (Ubuntu 13.01v)
Platform	:NS-2
Software	: Network Simulator 2.35
Programming languages	: Tool Command Lang., AWK, C++
FrontEnd	: OTCL (Object OrientedTool Command Language)
Tool	: Cygwin (to simulate in Windows OS)

IV. LITERATURE REVIEW RELATED TO EXISITNGWORK

A large number of researchers have worked on the topic, "*Design & Development of an effective key management in dynamic WSNs using certificate less-effective key management protocol for secure communications characterized by node mobility*". In this section, a brief review of the work done by various authors is being presented with their advantages & drawbacks.

Ying Qiu, Jianying Zhou, Joonsang Baek and Javier Lopez [50] have proposed an efficient and scalable protocol which establishes authentication keys between any pair of sensor nodes in a dynamic WSN. It is suitable for both static and dynamic WSNs. However, in a practical testing environment, theperformancedroppedsignificantlywhenthenumberofhops increases between two ends, which was a major drawback [6]. Seung-Hyun Seo, Jongho Won, Salmin Sultana and Elisa Bertino have proposed a certificate-less effective key management (CL-EKM) scheme for dynamic WSNs. However, the energy consumption is more that may degrade the network lifetime, which was a major drawback[7].

Xing Zhang, Jingsha He and Qian Wei proposed a distributed deterministic key management scheme for WSNs. This protocol consumes more storage in maintaining neighbour table if the network size increases. Since the neighbour table is limited to a threshold, sometimes a new trusted node may not be able to join the network, which was a major drawback in their paper [8]. Ramzi Bellazreg and Noureddine Boudriga have proposed a group key management protocol suitable for HWSNs. This protocol uses the secure tunnelling approach that ensures multiple nodes can communicate among them using the same tunnel. Intheir work, twomobilitymodelsofthetargetswereonlyconsidered&work was not carried out on multiple targets, which was a major drawback[9].

Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Chooworkedonthesecurityissuesusingblockchainfuturesin the IOT in WSNs. The authors surveyed articles presenting IoT security solutions for more than a decade & presented in their paper relating to the same. Optimization of bloc chains and block chain-based platforms were not dealt with, which was a major drawback[10].

 ©IJSRED:All Rights are Reserved

Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun, Abdul Sattar and Vijay Varadharajan worked on dynamic authentication schemes for hierarchical WSNs. The authors developed a security scheme for monitoring apps. One drawback of their scheme was that if the sensor nodes in one clusterchangefrequently,thegroupkeywillhavetobechanged as a result of which the transmission time increases [11]. Dynamic key distribution in WSNs with reduced communication overhead was researched upon by Ramu Kuchipudi, Dr. Ahmed Abdul Moiz Qyser & Dr. Balaram in their research paper presented in [12]. In order to protect the sensitive data in WSNs, secret keys were used to encrypt the exchanged messages between communicating nodes, thus projecting an effective method of key management in their paper.Onedrawbackintheirworktheymadeuseofonlycluster heads&consideredonlyveryfewnodesforthesimulation[12].

A hamming distance based dynamic key distribution scheme for WSN's was protocol was developed by Ramu Kuchipudi et.al. in [19]. A dynamic key management scheme for dynamic wireless sensor networks by Seyed Hossein Erfani et.al. in [13]. Their approach ensured that the 2 communicating nodes share at least one common key & also provided efficient ways for key generation and relocation as well as addition or deletion of mobile sensor nodes. One of the main drawback in their paper was the key distribution schemes used only one primarykeyandthus,compromiseofthiskeyleadstothefailure of the entire sensornetwork.

GaneshPathakandSuhasPatilworkedonthehybridnovel perspective of secure routing in WSNs in [20]. The main objective of their work was to extend the security of roaming nodes to attain the secure routing in the mobile networks. A Network Coding Approach to Secret Key Distribution was devised by Paulo Oliveira & João Barros in [21], where they consideredtheproblemofsecretkeydistributionusingmultiple scatteredsensornodes&amobiledevice(suchasalaptop)that could be used to bootstrap the network. Large distribution network was considered in their work where they considered different attacks on the node also [37]. The team also implemented the basic secret key distribution scheme on a sensor networking testbed, consisting of TelosB motes running the TinyOS 2.0 operating system. However, the authors did not work on the multihop secret key distribution, which was a part of their work[36].

JunqiZhangandVijayVaradharajanpresentedanewWSN securityschemebasedonlockschemeandemployeesID-based secure group key management [22]. Their scheme had several advantagesovertheavailableexistinglockschemes,wherebyit improved network's security system & thus minimized the no. of key storage requirements. A dynamic key management scheme by combining the advantages of simple cryptography and random key pre-distribution scheme was devised by Priyanka Goyal & her team in[23].

A novel dynamic key management scheme based on hamming distance for wireless sensor networks was devised by Divya & Thirumurugan in [24], where the author combined the features of simple cryptography and random key distribution schemes & thus, their work yielded effective results. Good security was also provided in their case. One drawback was the key size what they had used was 128 bits & no provision was made to work for higher bits.

A novel key management scheme was presented by Song Peng in [26], where in the keys are generated based on the relative node location & a non-negative irregular increasing function. In [25], the authors, Manel, Omar, Abid & Habib proposed a novel key management protocol for heterogeneous sensor networks based on pairing and identity based cryptography. Xiaojiang Du *et.al.* [27] presented an efficient cryptographic key management scheme for heterogeneous sensor networks using routing drive ECC concept.

A brief review of distributed dynamic key management schemes in wireless sensor networks was carried out by Seyed RezaNabavi&SeyedMortezaMousaviintheirsurveypaperin [28]. Their survey paper investigated into the special requirements of the distributed dynamic key management schemes in WSNs. They also gave the different key management schemes, with each one having its strengths, weaknesses and applications[13].

Jong-Myoung Kim *et.al.* worked on the energy efficient DKM's in the field of WSNs, wherein the authors proposed a key distribution scheme, based on exclusion-based systems and 't'degreebivariatepolynomials[29].In[30],theauthorsChun-Guang Ma *et.al.* discussed the heterogeneous WSNs group key management issues. One drawback in their work was when the degree of key graph was equal to four, the number of re-keying andtheencryptioncostareclosetooptimal,butwhenitexceeds 4, the protocol was not able to deliver goodresults.

It is a well-known fact the WSNs suffers a lot from the attacks & have got a lot of limitations and one has to design the protocol with a particular constraint only so as to achieve good efficiency [31]. A dynamic ID-based authentication scheme for M2M communication of healthcare systems was proposed by Tien-Dung Nguyen& Eui-Nam Huh in their research paper [46].

In majority of the work done by the various authors presented in the previous paragraphs, there were certain drawbacks / disadvantages / lacunas / demerits, which was presented at the end of the work done by each author. Some of the above mentioned drawbacks which were existing in the works done by the earlier researchers can be considered by the future researchers, their own problem can be defined & new algorithms can be developed in order to overcome some of the deficiencies of the existing algos.

Similartotheworkspresentedbyalargeno.ofresearchers in the preceding paragraphs, there were still quite a number of worksdonebymanyresearchersacrosstheworldtilldateinthe fieldofWSN.But,here,wehaveconsideredonlytheimportant ones [1]–[50] have been referred to herewith in the research work for some basic ideas for developing theprotocols.

 ©IJSRED:All Rights are Reserved

In majority of the work done by the various authors presented in the previous paragraphs, there were certain drawbacks / disadvantages / lacunas such as consideration of only the use of conventional methods, high compilation time, computationally very expensive, effect of attackers on the data sensor nodes were more, full-fledged automation of security deploymentnotdone,lessworkdoneonincreasingtheaccuracy & performance, real time implementation (h/w), very few people done, etc., pool size & number of sensors was medium, overheads of computation & transmission problems weremore, some developed protocol was not able to deliver good results, not energy efficient andscalable.

Some of the above mentioned drawbacks which were existing in the works done by the earlier researchers were considered in our research work & new algorithm is developed in order to overcome some of the deficiencies of the existing algos and also to develop some high efficient algorithms for increasing the security aspects during the data transmission in the networks from the source to the sink in-spite of vulnerable attacks from the attacking nodes. The research work was verified through effective simulation results done in the Network Simulator environment, thus substantiating the research problem undertaken.

V. REVIEW OF THE PROPSED RELATEDWORKS

Wireless sensor networks (WSNs) have been deployed for alargevarietyofapplicationsinvarioussectionofengineering, including military sensing and tracking, patient status monitoring, traffic flow monitoring, where sensory devices often move between different locations in the modern days. Encryption key protocols are required for securing data and for communications purposes. A certificate less-effective key management protocol (CL-EKMP) for secure data communication in dynamic WSNs characterized by theconcept of node mobility is being developed in this 1st contributory work. The CL-EKMP supports updates of the efficient keys, whenever a sensor node leaves a cluster or joins a cluster, thus ensuring forward and backward keysecrecy.

The developed protocol also supports efficient key revocation concepts for compromised nodes & minimizes the impact of any general purpose sensor node, which can be compromised on the security of other communication links & its layers. A security analysis of the developed work was also carried out by us by developing protocols and the developed schemeshowsthattheprotocoliseffectiveindefendingagainst vulnerable attacks, intruders, hackers & data corruptions. The certificate less-effective key management based protocol in Ubuntu OS is formulated and then simulated using the NS-2 simulatortoassessforvariousnetworkparameterssuchastime, energy, communication, and memory performance of the dynamicm-WSNs.

Dynamic wireless sensor networks (WSNs), which enable mobility of sensor nodes, facilitate wider network coverageand more accurate service than static WSNs. Therefore, dynamic WSNs are being rapidly adopted in monitoring applications, suchastargettrackinginbattlefieldsurveillance,healthcare systems, traffic flow and vehicle status monitoring, dairy cattle health monitoring. However, sensor devices are vulnerable to malicious attacks such as impersonation, interception, capture or physical destruction, due to their unattended operative environments and lapses of connectivity in wireless communication. Thus, security is one of the most important issues in many critical dynamic WSN applications.

Whenever and wherever the nodes move, the dynamic WSNs needs to address the key security requirements, such as nodeauthentication,dataconfidentialityandintegrityinthedata transmissions from the source to the sink. Encryption key management protocols for dynamic m-WSNs have been proposed by few authors in the past based on symmetric key encryptiontoaddressthedifferenttypesofsecurityissuesinthe WSNs. Because of their limited energy and processing capability, such type of encryption is well-suited for the sensor nodes.

But, one drawback is, it suffers from high communication overheads&thusrequiresalargememoryspacetostoreshared pair wise keys at the same time increasing the compilation time of data transmission from the source to the sink. Moreover, itis alsonotscalableandnotresilientagainstcompromisesandthus it is unable to support the different static & mobile node mobilities. Because of the above mentioned problems, the symmetric key encryptions are not definitely suitable for dynamic mobile wireless sensor networks. Moreover, security protocols with & without keying takes a lot of time to send the data packets to the base station, which is taken care of in our research work in an efficientmanner.

Asymmetric key based approaches have been proposed for dynamic WSNs by many researchers across the world in the recent days. The asymmetric key based approaches takes the advantage of public key cryptography (PKC) such as elliptic curve cryptography (ECC) or identity-based public key cryptography (ID-PKC) in order to simplify the key establishments and also the data authentication between different nodes. When computation cost & data transportation comes into picture, the PKC is relatively more expensive than the symmetric key encryption. But, more recent improvements that are done in the implementation of ECC have showed the feasibility of applying public key cryptography to the dynamic m-wireless sensor nets.

Moreover, public key cryptography is more resilient to node compromise attacks & is scalable and flexible quantitatively (more in nature). However, it was found from variousliteraturesthatthesecurityweaknessesofexistingECC-based schemes approaches are more vulnerable / susceptible to message forgery, vulnerable attacks, key compromise and known-key attacks by the intruders. Also, the critical security flaws of that the static private key that was exposed to theother sidesofthenetworkwhenbothnodesestablishthesessionkeys were analyzed in greater detail by couple of network researchers.

In fact, these ECC-based schemes with certificates when it was applied directly to the dynamic WSNs, they suffered from

 ©IJSRED:All Rights are Reserved

thecertificatemanagementoverheadsoftheentiresensornodes, asaresultofwhichtherearenotsuitabletopracticalapplication problems that too for large scale m-WSNs. Due to the computational overhead for pairing operations, the pairing operation based ID-PKC schemes become moreinefficient.

Tothebestofourknowledgeaftercarryingoutanextensive literaturesurvey,efficientandsecurekeymanagementschemes fordynamicWSNsstillhavenotyetbeenproposedeventilldate because of a large number of network drawbacks, limitations, dis-advantages, etc. Because of the previously mentioned drawbacks, we have resorted to develop an effective key management in dynamic WSNs using CL-EKMP for secure communications characterized by node mobilityconcept.

VI. EXISTING WSNSYSTEMS

In the following paragraphs, couple of authors who have worked on the CL-EKMP concepts have been portrayed. A brief details about the existing systems are being portrayed. Al-Riyami and Paterson introduced a newconcept in CL-EKMP & made the concept of certificate less public key cryptography (CL-PKC)asavirtualsimulatedmodelfortheuseofpublickey cryptography.Thisconceptwhichtheyhavedevelopedavoided the inherent escrow of identity-based cryptography and did not require certificates to guarantee the authenticity of public keys in the different layers of the WSNs. This concept has beenused by us with certainmodifications.

A principal certificate-less successful key management convention (CL-EKM) for secure correspondence in element WSNswasproposedbyArunaKumar&SaiPriyain[48].Their algo underpins proficient correspondence for key upgrades and management when a node leaves or joins a cluster and subsequently guarantees forward and in reverse key mystery & theirplanwasversatileagainstnodecompromises,thusyielding good results.

The lack of certificates and the presence of an adversary who has access to a master key necessitated the careful development of a new security model by them, which yielded excellentresults.Intheirwork,theuser'sfullprivatekey(FPK) wasacombinationofapartialprivatekey(PPK)generatedbya key generation center (KGC) & the user's own secret value. Further, the special organization of the full private/public key pair removed the need for certificates and also resolved the key escrow problem by removing the responsibilities for the user's full privatekeys.

Elliptic curve cryptography (ECC) based certificate less hybrid sign-cryption scheme without pairing of the keys was proposed by Seo & Beritno in their research paper in [7]. The pair wise key of CL-EKMP could be efficientlyshared between 2nodesw/orequiringtaxingpairingoperations&theexchange of certificates because of the properties of CL-HSC. Tosupport the node mobility, their work 'CL-EKM' also supported lightweight processes for cluster key updates upon execution whenanodemovesandkeyrevocationisexecutedwhenanode isdetectedasmaliciousorleavestheclusterheadspermanently. CL-EKM was also scalable in caseof additions of new nodes after the wireless sensor network deployment. CL-EKM was also secured against node compromise, cloning and impersonation&thusensuredforwardandbackwardsecrecyof thedatas.

Atwo-layeredkeymanagementschemeandadynamickey update protocol in dynamic WSNs based on theDiffie-Hellman (DH) was proposed by Agrawal, Roman, Das, Mathuria & Lopez [6] in their research paper [50]. However, both schemes werenotsuitedforsensorswhichwerehavinglimitedresources and were unable to perform expensive computations with large key sizes for more than 1KB. An ECDSA scheme to verify the identity of a cluster head and a static EC-Diffie-Hellman key agreementschemetosharethepairwisekeybetweenthecluster heads was developed by the team of Du, Xiong and Wang in theirwork.

When it was carefully analyzed, the scheme by Du et.al. [44]wasnotsecuredagainstknown-keyattacksbecausethepair wise key between the cluster heads was static in nature andwas not dynamic. But, the team of Du et.al. used a modular arithmetic-based symmetric key approach to share the pairwise keys between a sensor node and a cluster head. It was justified thatasensornodecouldnotestablishapairwisekeywithother sensor nodes directly, but, it required the support of the cluster heads. The authors developed forward and backward secrecy to the data by using a key update process whenever a new node joinstheclusterorwheneveranodeiscompromised.Onemajor drawback of this approach was that it did not provide a process to protect against clone and impersonation attacks by the attacker node [44].

Encryption key management protocols for dynamic WSNs have been developed in the past based on symmetric key encryption by many authors in order to address the security issues in the networks. Such type of encryptions were well-suited for sensor nodes only because they were having limited energy, processing & computing capabilities. The drawbacks were it was suffering from very high communication overhead andthusrequiredalargememoryspacetostoresharedpairwise keysandalso.Moreover,itwasalsonotscalable&notresilient against compromises and was unable to support the node mobilities inWSNs.

Therefore, symmetric key encryption was not suitable for dynamic m-WSNs. More recently, asymmetric key based approaches have been proposed for dynamic WSNs. These approaches took undue advantage of public key cryptography (PKC) such as elliptic curve cryptography (ECC) or identity-based public key cryptography (ID-PKC) in order to simplify thekeyestablishmentsanddataauthenticationbetweendifferent sensornodes.

Huang et.al. worked on the fast authenticated key establishment protocols for self-organizing sensor networks in [35]. Liu and Ning worked on the configurable library for elliptic curve cryptography in wireless sensor networks in [26] and developed a library which was stored in the kernels which could be used for further applications [43]. Du et.al. developed an efficient key management scheme for WSNs in [44].

 ©IJSRED:All Rights are Reserved

Lin & Shun worked on the cryptanalysis and improvement ofadynamicandsecurekeymanagementmodelforhierarchical heterogeneous sensor networks in their research paper in [36]. Szczechowiak et.al. did extensive research work on the testing the limits of elliptic curve cryptography in sensor networks & produced good results [37]. An improved ID-based key management scheme in wireless sensor network was developed byChaterjee&Guptain[38]andshowedthattheirdatatransfer will be a success in spite ofattackers.

Rassam did a survey of intrusion detection schemes in wireless sensor networks in [40], which provided a base for many of the researchers to define their research problem statement after a thorough study of the WSNs. Similarly, Paradis & Han did an extensive survey of fault management in WSNs, which also provided a base for many of the researchers todefinetheirresearchproblemstatementsinthefieldofWSNs. Zhu et.al worked on the detection of node replication attacks in mobile sensor networks [39], which was used by us in our research work with the attacker node trying to corrupt the data whichisbeingsentfromthesourcetothesink.Jiangdeveloped a new method for node fault detection in wireless sensor networks in [41]. The drawbacks or the lacunas in the existing systemswere

- Symmetric key encryption suffers from high communication overhead and requires large memory space to store shared pair wisekeys.
- Itisalsonotscalableandnotresilientagainstcompromises, and unable to support nodemobility.
- The pairing operation based ID-PKC schemes are inefficient due to the computational overhead for pairing operations.
- PKC was relatively more expensive than symmetric key encryption wr.t. the computationalcosts.

VII. DEVELOPED WSN SYSTEMMODEL

In the 1st contributory work, the development of an effectivekeymanagementindynamicwirelesssensornetworks using CL-EKM protocol for secure communications characterized by node mobility is presented here incorporating some of the drawbacks of the work done by earlier researchers in the developed model. After the incorporation, efficient algorithms are developed in the 1st contributory work. Here in this #C1, a certificate less effective key management protocol (CL-EKMP) scheme for dynamic WSNs is being presented ina nut-shell.

In this certificate less public key cryptography protocol scheme (CL-PKCP), the user's full private key will be a full combination of a partial private key (PPK) generated by a key generation center (KGC) & the user's own secret value (OSV). The special organization of the full private / public key pair removestheneedforcertificates&alsoresolvesthekeyescrow problem by removing the responsibility for the user's full private key. The benefit of ECC keys defined on an additive group with a 160-bit length as secure as the RSA keys with 1 KBlengthisalsotakencareof.Inordertodynamicallyprovide both node authentication and establish a pair wise keybetween nodes, a CL-EKM protocol scheme by utilizing a pairing-free certificate less hybrid signcryption scheme (CL-HSC) is being developed.

Due to the properties of CL-HSC, the pair wise key of CL-EKM can be efficiently shared between two nodes without requiring taxing pairing operations and the exchange of certificates. To support node mobility, the developed CL-EKM also supports lightweight processes for cluster key updates executed when a node moves, and key revocation is executed when a node is detected as malicious or leaves the cluster permanently. CL-EKM is scalable in case of additions of new nodes after network deployment. CL-EKM is secure against node compromise, cloning and impersonation, and ensures forward and backward secrecy. The security analysis of the developed scheme shows its effectiveness, which can be seen from the simulated results presented in the simulation results section.

The developed system consist of sender, a network with 6 cluster heads having a group of

- sensornodes,
- a receiver or a base station&
- network(cluster)
- 2 attackingnodes,

which are explained one after the other as follows.

A. Sender

The sender will browse the data file and then send to the particular receivers. Sender will send their data file to network and forms clusters, in a cluster highest energy sensor node will be activated and send to particular receiver (A, B, C…) and if any attacker will change the energy of the particular sensor node, then sender will reassign the energy for sensor node.

B. Network

Network will accept the file from the sender, the cluster headwillselectfirstanditsizewillreducedaccordingtothefile size, then next time when we send the file, the other node will be cluster head.

C. Cluster

In cluster n-number nodes are present and the clusters are communicates with every clusters (cluster-1 to cluster-6). In a clusterthesensornodewhichhavemoreenergyconsideredasa clusterhead.Thesenderwillassigntheenergyforeach&every node. The sender will upload the data file to the network; in a network clusters are activated and the cluster-based networks, to select the highest energy sensor nodes, and send to particular receivers.

D. Receiver(BS)

The receiver can receive the data file from the sender via network. The receivers receive the file by without changing the File Contents.

 ©IJSRED:All Rights are Reserved

E. CL-EFKM ProtocolUsed

consists of Network Model, Pairwise Key Generation, Cluster Formation & Key Update (pair-wise & cluster key).

F. NetworkModel

The network consists of a number of stationary or mobile sensor nodes and a BS that manages the network and collects data from the sensors. Sensor nodes can be of two types -nodes with high processing capabilities, referred to as H-sensors and nodeswithlowprocessingcapabilities,referredtoasL-sensors. Nodesmayjoinandleavethenetwork,andthusthenetworksize may dynamically change. The H-sensors act as cluster heads while L-sensors act as cluster members. They are connected to the BS directly or by a multi-hop path through other H-sensors. H-sensors and L-sensors can be stationary ormobile.

G. Pairwise KeyGeneration

The advertisement message contains its identifier and public key. At first, two nodes set up a long-term pairwise master key between them, which is then used to derive the pairwise encryption key.

H. ClusterFormation

Once the nodes are deployed, each H-sensor discovers neighbouringL-sensorsthroughbeaconmessageexchangesand then proceeds to authenticate them. If the authentication is successful, the H-sensor forms a cluster with the authenticated L-sensors and they share a common cluster key. The H-sensor alsoestablishesapairwisekeywitheachmemberofthecluster.

I. Key Update : Pairwise KeyUpdate

To update a pairwise encryption key, two nodes which shared the pairwise key perform a Pairwise Encryption Key Establishment process.

J. Key Update : Cluster KeyUpdate

OnlyclusterheadH-sensorscanupdatetheirclusterkey.If an L-sensor attempts to change the cluster key, the node is considered a maliciousnode.

VIII. SIMULATION RESULTS &EXECUTIONSTEPS

The coding (script writing) for the key management in dynamic wireless sensor networks using CL-EKM protocol for secure communications characterized by node mobility is developedinthe.Clanguageandonceitiscompleted,itistested foritseffectivenessasperthealgostepsgivenbelowfroms1to s12. The Network Simulator (NS-2) tool is being used to dothe simulation.

1. The coding is done in the **.**tcl scripting incorporating the developed CL-EKM protocol.
2. The developed code is saved in a particular folder in the Ubuntuenvironment.
3. Ubuntu isstarted.
4. At the terminal, commands like sudo –s is being used to enter thekernel.
5. Password is beingset.
6. Thesourcecodeinwhichthedirectory/folderispresentis changed using cd command.
7. The code is run using nsfilename**.**tcl
8. The command window of the NS-2 simulator appears with the simulator start button along with the network animator (Fig.5).
9. Once the simulation is started, the sensor node deployment within the 8 cluster heads along with the base station, sink, source, etc…. & the 2 attacker nodes appears on the NS-2 animator screen (Fig. 6).
10. Data transfer starts from the source (normally 0), nodes starts sending & receiving the data packets after thekeying process, once the security key is verified (Fig.7).
11. Simulation takes couple of minutes, passes different stages of data packets sending, verification, encryption, decryption from the source to the sink (Figs. 8 to14).
12. Oncethedatatransferisfullysuccessful,allthenodesturns red indicating the 100 % success rate (Fig.8.15).
13. Results are observed at the command prompt (terminal) by using the results visualizations chmod 777 results.sh& ./results.sh (Fig. 16).
14. Output graphs of showing the number of keys stored in the L-sensor (cluster heads) is observed with a simulation step size of 5 ms (Fig.17).
15. Simulationresultofno.ofsurvivalnodesoverroundsw.r.t. time, is observed next showing the reduction in timings with security keying (taking 22 secs – red color) & taking 28 seconds w/o security keying authentication of the nodes (green color), thus showing the effectivity of the proposed methodology (Fig.18).

IX. ADVANTAGES OF DEVELOPEDMETHODOLOGY

The advantages of the work is presented as follows ….

- The works shows how the security weaknesses of existing ECC based key management schemes for dynamic WSNs can be overcomedwith.
- A number of efficient key management procedures can be defined as supporting node movements across the different clusternodes.
- The key revocation process for compromised nodes can be implementedwith.
- The proposed certificate less - effective key management scheme (CL-EKMS) is lightweight and hence suitable for the dynamic wireless sensornetworks.
- The proposed scheme is resilient against any type of node compromise, cloning, infiltration and impersonation attacks.
- The protection of the data confidentiality and integrity duringthetimeofdatatransmissionisachievedwithagood successrate.
- Provides more security & decreases theoverhead.
- Protects the data confidentiality and integrity to theWSNs

 ©IJSRED:All Rights are Reserved

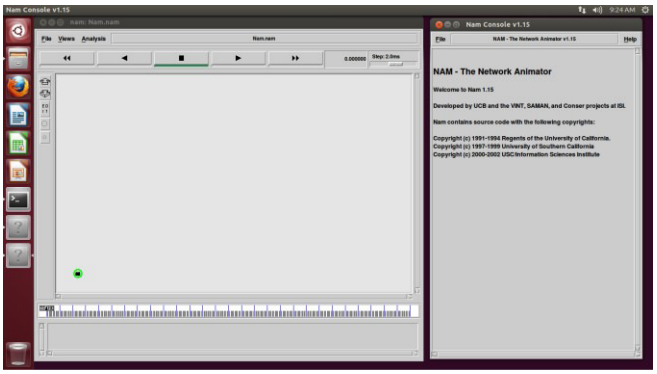

Fig. 5 : Network simulator / animator front screen panel from where the simulation can be started by pressing forward button (4th from top)

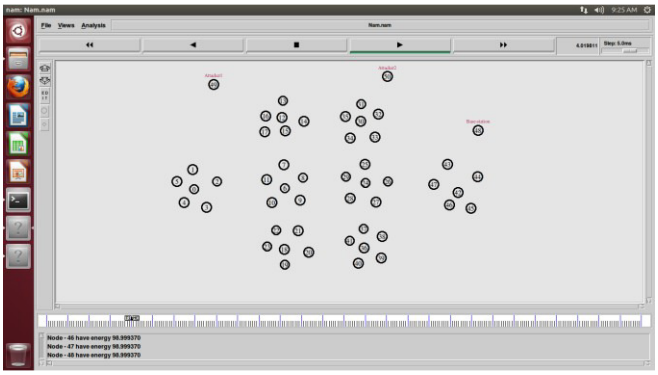

Fig. 6 : Sensor node deployment within the 8 cluster heads along with the base station, sink, source, etc…. & the 2 attacker nodes (after the simulation is started)

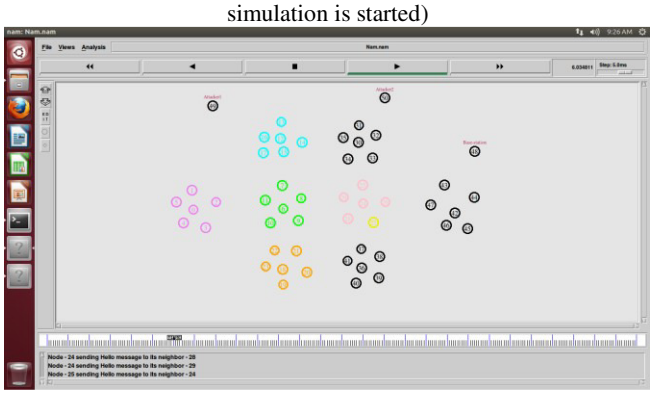

Fig. 7 : Data transfer taking place from the source to the sink after the keys in the cluster heads gets authenticated / verified after the key verification process (below box-sending messages to the neighbouring sensor nodes)

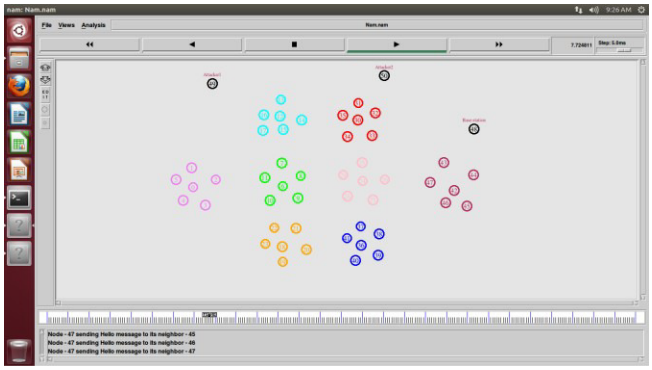

Fig. 8 : Node authentication process & data transfer going on (mid-way stage)

Fig. 9 : Node authentication process & data transfer going on (mid-way stage) with broadcasting the messages to the sensor nodes

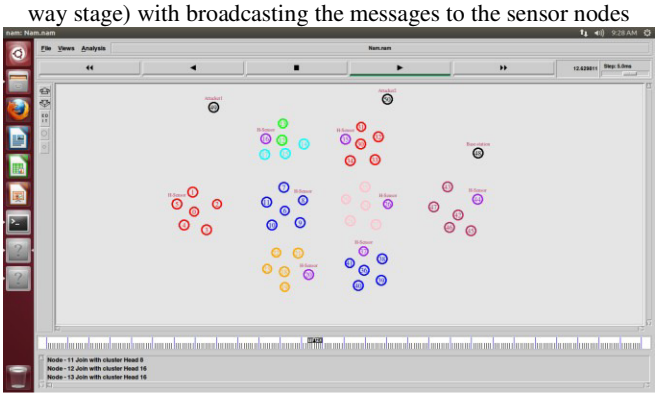

Fig. 10 : Data transfer messages transmission process going on(mid-way stage) with the cluster heads – intermittentstage

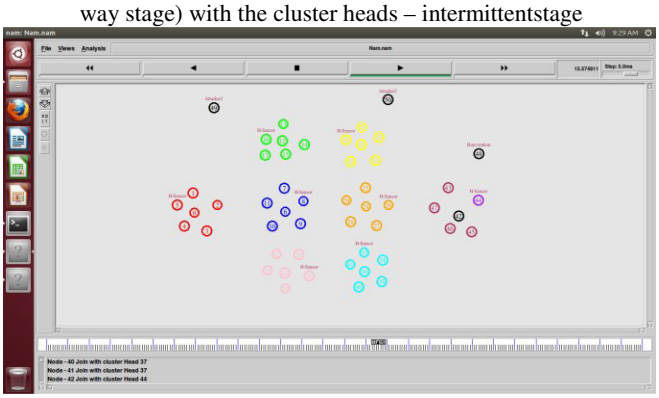

Fig. 11 : Data transfer messages transmission process going on(mid-way stage) with the cluster heads – intermittentstage

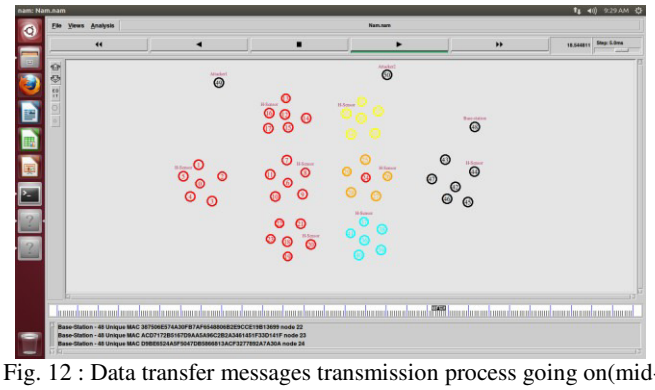

Fig. 12 : Data transfer messages transmission process going on(mid-way stage) with the cluster heads – intermittentstage

 ©IJSRED:All Rights are Reserved

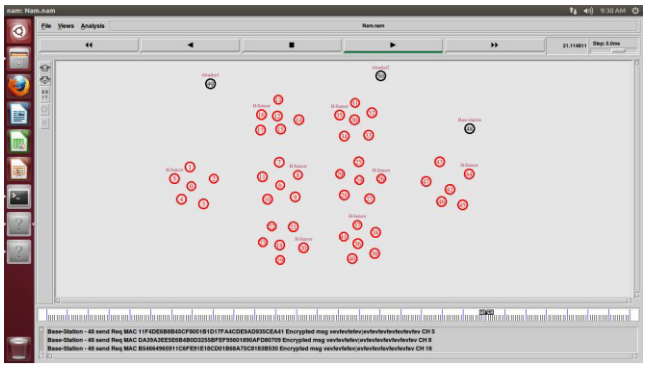

Fig. 13 : Data transfer messages transmission process going on(mid-way stage) with the cluster heads – intermittentstage

Fig. 14 : Data transfer messages transmission process going on(mid-way stage) with the cluster heads – intermittentstage

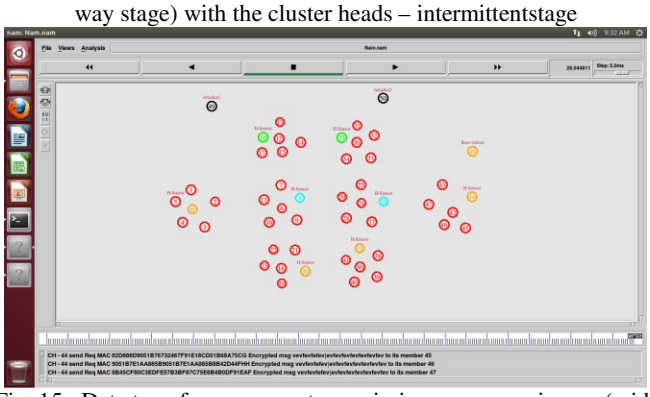

Fig. 15 : Data transfer messages transmission process going on (mid-way stage) with the cluster heads – intermittent stage ……. end of the simulation (see the cursor moved fully to the right), data being transferred from the source (sensor node 0) to base station (node 48)

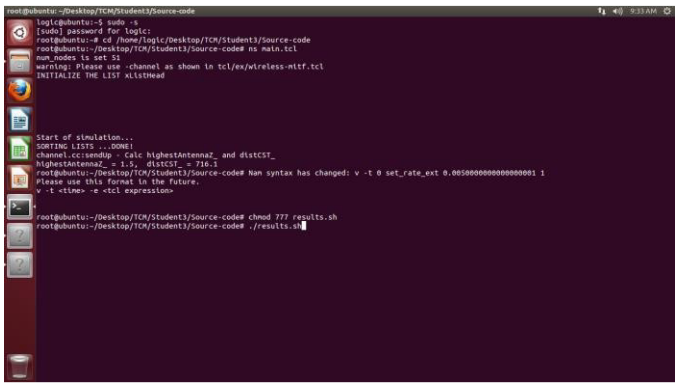

Fig. 16 : Commands used at the terminal to see the results of the simulation once the data transfer from the source to the sink is over

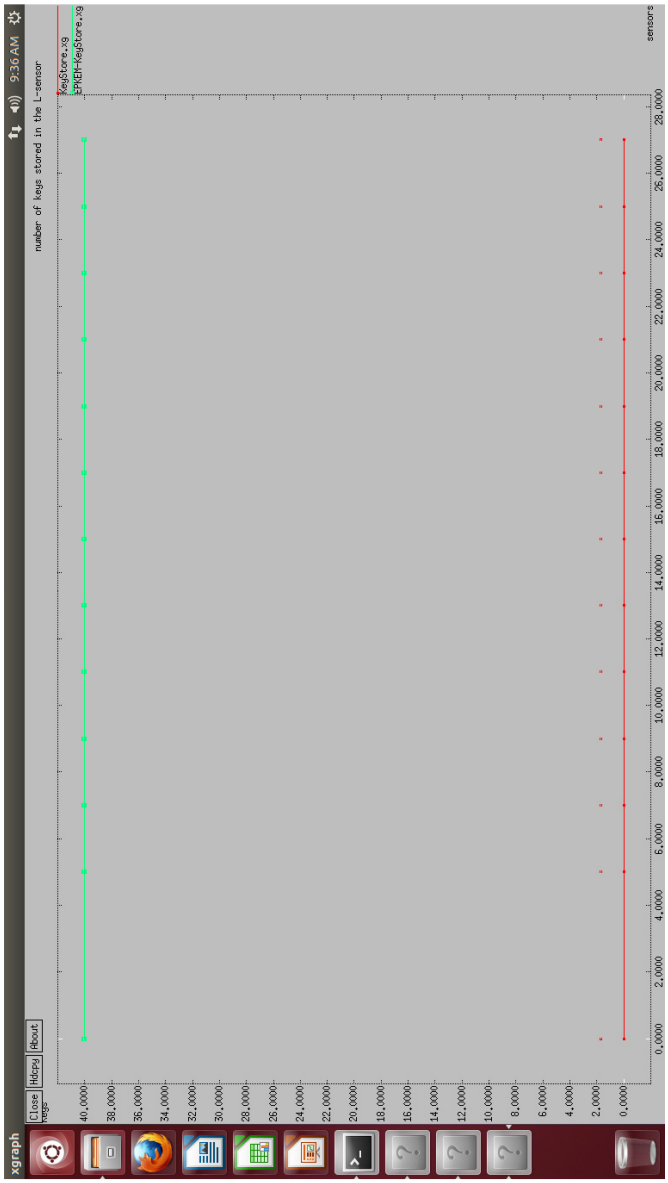

Fig. 17 : Simulation result showing the number of keys stored in the L-sensor, time taken to complete the simulation 28 mins with step size of 5 ms.

 ©IJSRED:All Rights are Reserved

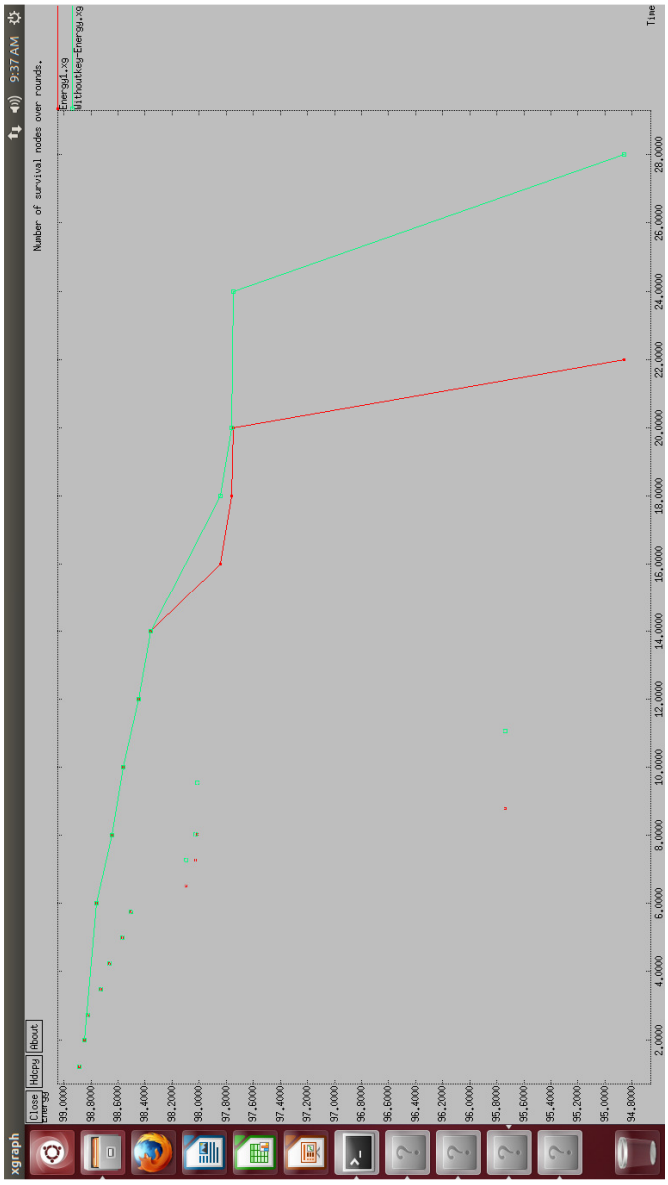

Fig. 18 : Simulation result of no. of survival nodes over rounds w.r.t. time, our proposed work showing reduction in timings with security keying (taking 22 secs – red color) & taking 28 seconds w/o security keying authentication of the nodes (green color)

X. CONCLUSION

Research was carried out on the development of enhanced securekeymanagementframeworkindynamicmobilewireless sensor networks. In this paper, the design & development of an effective key management in dynamic WSNs using Certificate-LessEffectiveKeyManagement(CL-EKM)protocolforsecure communications characterized by node mobility is being presented. The simulation results shows the effectivity of the methodology adopted. It is inferred that if the key (similar to the OTP in mobile) concept is used to authenticate the node, then security level increases and the data packets are send in lesser time because of no intervention of the mis-behaving nodes. One novel contributory work (#C1) was carried out duringthecourseoftheresearchworktilldateinthefieldof securitykeyingaspectsinWSNsandgoodresultswereobtained eveninthepresenceoftheattackernodestryingtohackthedata transmission, while the datas are being transmitted from the source to the destination.

Codes were developed in NS-2 environment for the said contributory work, the program was run & the results were observed.Itwasobservedthatthenetworktookoptimaltimefor the transmission of data & even though the attackers are trying to corrupt the data transmission process, the process is not get corrupted as such effective security measures have been taken during the transmission process. It was observed that w/o the security keying, the simulation took 28 mins, but with the securitykeydeploymentusingtheCL-EKMprotocolforsecure communications characterized by node mobility, the data transfer took only 22 mins, thus showing the effectivity of the key authentication process w.r.t. data transfer schemes in wireless sensor mobilenetworks.

REFERENCES

[1] Majid I. Khan, Wilfried N. Gansterer, Guenter Haring, "Static vs. mobile sink : The influence of basic parameters on energy efficiency in wireless sensor networks", *Comp. Communications*, Vol. 36, No. 9, pp. 965–978, May2013.

[2] https://en.wikipedia.org/wiki/Mobile_wireless_sensor_network

[3] https://en.wikipedia.org/wiki/Wireless_sensor_network

[4] http://www.ni.com/white-paper/7142/en/

[5] Xiaobing He, Michael Niedermeier, Hermannde Meer, "Dynamic key management in wireless sensor networks: A survey", *Jour. of Network & Comp. Applications*, Vol. 36, Issue 2, pp. 611-622, Mar.2013.

[6] Qiu Ying, Zhou, Jianying, Baek, Joonsang, and Lopez, Javier, "Authentication and key establishment in dynamic wireless sensor networks", *Jour. of Sensors*, ISSN 1424-8220, Vol. 10, No. 4, pp. 3718-3731,2010.

[7] Seung-Hyun Seo, Jongho Won, Salmin Sultana and Elisa Bertino, "Effective Key Management in Dynamic Wireless Sensor Networks", *IEEE Trans. on Info. Forensics & Security*, Vol. 10, No. 2, pp. 371 – 383, Feb.2015.

[8] Xing Zhang, Jingsha He and QianWei, "EDDK: Energy-Efficient Distributed Deterministic Key Management for Wireless Sensor Networks",*HindawiPublishingCorporationEURASIPJour.onWireless Communications & Networking*, Vol. 2011, pp. 1-11, Article ID 765143, 2011.

[9] Ramzi Bellazreg and Noureddine Boudriga, "DynTunKey : a dynamic distributed group key tunnelling management protocol for heterogeneous wireless sensor networks", *EURASIP Jour. on Wireless Comm. & Networking*, paper id 2014:9, pp. 1-19,2014.

[10] Mandrita Banerjee, Junghee Lee, Kim-Kwang Raymond Choo, "A block chain future for internet of things security: a position paper", *Elsevier's Dig. Comm. & Networks*, Vol. 4, pp. 149–160,2018.

[11] JunqiZhang,RajanShankaran,MehmetA.Orgun,AbdulSattarandVijay Varadharajan, "A Dynamic Authentication Scheme for Hierarchical Wireless Sensor Networks", *Mobile & Ubiquitous Systems : Computing, Networking & Services*, 7th *Int. ICST Conf., MobiQuitous-2010*, Tokyo, Japan, Dec. 2–4,2013.

[12] RamuKuchipudi,Dr.AhmedAbdulMoizQyser,Dr.V.V.S.S.SBalaram, "A Dynamic Key Distribution in Wireless Sensor Networks with reduced communicationoverhead",*Int.Conf.onElectr.,Electron.&Optimization Techniques* (ICEEOT) – 2016, pp. 3651-3654, Chennai, Tamil Nadu, India, 3-5 Mar.2016.

[13] Seyed Hossein Erfani, Hamid H.S. Javadi and Amir Masoud Rahmani "A dynamickeymanagementschemefordynamicwirelesssensornetworks", *Security & Comm. Networks*, Vol. 8, No. 6, pp. 1040–1049, Jun. 2014, Apr. 2015.

 ©IJSRED:All Rights are Reserved

[14] Eschenauer L., Gligor V.D., "A key-management scheme for distributed sensor networks", *Proc. of the 9th ACM Conf. on Comp. & Comm.*, Sec., ACM, Washington, DC, USA, pp. 41–47,2002.

[15] Çamtepe S.A., Yener B., "Combinatorial design of key distribution mechanisms for wireless sensor networks", *IEEE / ACM Trans. on Networking*, Vol. 15, No. 2, pp. 346–358,2007.

[16] Lee J., Stinson D.R., "On the construction of practical key pr-distribution schemes for distributed sensor networks using combinatorial designs", *ACM Trans. on Info. & Syst. Sec.*, Vol. 11, No. 2, pp. 1–35,2008.

[17] Ruj S., Roy B., "Key pre-distribution using partially balanced designs in wireless sensor networks", *Jour. of Parallel & Distributed Processing & Apps.,* Springer - Berlin Heidelberg, pp. 431–445,2007.

[18] DongJ.W.,PeiD.Y.,WangX.L.,"Aclassofkeypre-distributionschemes based on orthogonal arrays", *Jour. of Comp. Sci. & Tech*, Vol. 23, No. 5, pp. 825–831,2008.

[19] Ramu Kuchipudi, K. Vaishnavi Prapujitha, Y.G Shantha Reddy, "A HammingDistanceBasedDynamicKeyDistributionSchemeforWireless Sensor Networks", *Int. Jour. of Engg. & Comp. Sci.*, ISSN : 2319-7242, Vol. 2, No. 11, pp. 3197-3201,2013.

[20] Ganesh R. Pathak and Suhas H. Patil, "A Hybrid Novel Perspective of Secure Routing in Wireless Sensor Networks", *Indian Jour. of Sci. & Tech.*, Vol. 9, No. 10, pp. 1-8, Mar.2016.

[21] PauloF.Oliveira,JoãoBarros,Member,"ANetworkCodingApproachto Secret Key Distribution", *IEEE Trans. on Info. Forensics & Sec.*, Vol. 3, No. 3, pp. 414-423, Sept.2008.

[22] Junqi Zhang and Vijay Varadharajan, "A New Security Scheme for Wireless Sensor Networks", *IEEE GLOBECOM-2008, IEEE Global Telecom. Conf.*, New Orleans, LO, USA, pp. 1-5, 30 Nov-4 Dec.2008.

[23] PriyankaGoyal,Dr.MukeshKumar,RituSharma,"ANovelandEfficient dynamic Key Management Technique in Wireless Sensor Network", *Int. Jour. on Adv. Networking & Apps.*, ISSN : 0975-0290, Vol. 4, No. 1, pp. 1462-1466,2012.

[24] R. Divya , T. Thirumurugan, "A Novel Dynamic Key Management Scheme Based On Hamming Distance for Wireless Sensor Networks", *Int.Jour.ofScientific&Engg.Res.*,ISSN2229-5518,Vol.2,Issue5,pp. 1-7, May2011.

[25] Manel Boujelben, Omar Cheikhrouhou, Mohamed Abid, Habib Youssef, "A Pairing Identity based Key Management Protocol for Heterogeneous Wireless Sensor Networks", *IEEE Int. Conf. on Network & Service Security*, ESR Groups Paris, France, pp. 1-5, 24-26 June2009.

[26] SongPeng,WenjuLiu,ZeWangandYanfenZhang,"APower-dependent KeyManagementSchemeforWirelessSensorNetwork",*8thInt.Conf.on Wireless Comm., Networking & Mobile Computing*, Shanghai, China, pp. 1-4, 21-23 Sep.2012.

[27] Xiaojiang Du, Mohsen Guizani, Yang Xiao, Hsiao-Hwa Chen, "A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks", *IEEE Trans. on Wireless Comm.*, Vol. 8, No. 3, pp. 1223-1229, Mar.2009.

[28] SeyedRezaNabavi&SeyedMorteza,"AReviewofDistributedDynamic Key Management Schemes in Wireless Sensor Networks", *Jour. of Computers*, Vol. 13, No. 1, pp. 77-89, Jan.2018.

[29] Jong-Myoung Kim, Joon-Sic Cho, Sung-Min Jung, and Tai-Myoung Chung, "An Energy-Efficient Dynamic Key Management in Wireless Sensor Networks", *The 9th Int. Conf. on Adv. Comm. Tech.*, Okamoto, Kobe, Japan, Vol. 3, pp. 2148 – 2153, 12-14 Feb.2007.

[30] Chun-Guang Ma, Jiu-Ru Wang, Hua Zhang, Zhen-Jiang Chu, "An Efficient Group Key Management Protocol for Heterogeneous Sensor Networks", *IET Int. Conf. on Wireless Sensor Networks 2010,* IET-WSN 2010, 280 – 285, Beijing, China, 15-17 Nov.2010.

[31] Vaishali Patel & Jaydeep Gheewala, "An efficient session key management scheme for cluster based wireless sensor networks", *IEEE Int. Adv. Computing Conf.* (*IACC*), Bangalore, India, pp. 963-967, 12-13 Jun.2015.

[32] Dr.SunilkumarS.Manvi&Dr.MahabaleshwarS.Kakksageri,"Wireless & Mobile Networks – Concepts & Protocols", *Wiley India Pvt. Ltd. Publications*, New Delhi, India, ISBN, 978-81265-5855-1, 2nd Edn., 475 Pages, 2016.

[33] Haijun L.andChaoW.,"AnEnergyEfficientDynamicKeyManagement Based Polynomial and cluster in wireless sensor networks", Jour. of Convergence Info. Tech., Vol. 6, No. 5, pp. 321-328, May2011.

[34] Yang, Shuang-Hua, "Wireless Sensor Networks - Principles, Design and Applications", *Springer*,2014.

[35] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks", *Proc. 2nd ACM Int. Conf. WSNA*, pp. 141–150,2003.

[36] Oliveira X.J. Lin and L. Sun, "Cryptanalysis and improvement of a dynamic and secure key management model for hierarchical heterogeneoussensornetworks",Proc.IACRCryptol.ePrintArchive,pp. 698–698,2013.

[37] P. Szczechowiak, L.B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC : Testing the limits of elliptic curve cryptography in sensor networks", *Proc. 5th Eur. Conf. WSN*, Vol. 4913, pp. 305–320,2008.

[38] K. Chatterjee, A. De, and D. Gupta, "Animproved ID-based key management scheme in wireless sensor network", *Proc. 3rd Int. Conf. ICSI*, Vol. 7332, pp. 351–359,2012.

[39] W.T. Zhu, J. Zhou, R.H. Deng, and F. Bao, "Detecting node replication attacks in mobile sensor networks: Theory and approaches", *Jour. Secur. Commun. Netw.*, Vol. 5, No. 5, pp. 496–507,2012.

[40] M.A. Rassam, M.A. Maarof and A. Zainal, "A survey of intrusion detection schemes in wireless sensor networks", *Amer. J. Appl. Sci.*, Vol. 9, No. 10, pp. 1636–1652,2012

[41] P. Jiang, "A new method for node fault detection in wireless sensor networks", Jour. of Sensors, Vol. 9, No. 2, pp. 1282–1294,2009.

[42] L. Paradis and Q. Han, "A survey of fault management in wireless sensor networks",*Jour.Netw.Syst.Manage.*,Vol.15,No.2,pp.171–190,2007.

[43] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks", *Proc. Int. Conf. on IPSN*, pp. 245–256, Apr.2008.

[44] D.Du,H.XiongandH.Wang,"Anefficientkeymanagementschemefor wireless sensor networks", *Int. J. Distrib. Sensor Netw.*, Vol. 2012, Art. ID 406254, Sep.2012.

[45] Ibrahiem M. M. El Emary, S. Ramakrishnan, "Wireless SensorNetworks : From Theory to Applications", *1st Edition*, CRC Press, *Published* Nov.16, 2016, 799 Pages, ISBN 9781138198821 - CAT# K31414.

[46] Tien-Dung Nguyen & Eui-Nam Huh, "A dynamic ID-based authentication scheme for M2M communication of healthcare systems", *TheInt.ArabJour.ofInfo.Tech.*,Vol.9,No.6,pp.519-511,Nov.2012.

[47] Ali Idarous Adnan, Zurina Mohd Hanapi, Mohamed Othman, Zuriati AhmadZukarnain,"ASecureRegion-BasedGeographicRoutingProtocol (SRBGR) for Wireless Sensor Networks", *Jour. Plos One*, DOI:10.1371/journal.pone.0170273, Vol. 12, Issue 1, Jan. 25,2017.

[48] P. Aruna Kumari & V. Sai Priya, "Energy Efficient Dynamic Wireless Sensor With Certificate Less Effective Key Management Protocol For Secure Communications", *Int. Jour. of Sci. Engg. & Adv. Tech.*, IJSEAT, Vol. 5, Issue 2, ISSN 2321-6905, February2017.

[49] S.U. Khan, C. Pastrone, L. Lavagno and M. A. Spirito, "An energy and memory-efficient key management scheme for mobile heterogeneous sensor networks", *Proc. 6th Int. Conf. CRiSIS*, pp. 1–8, Sep.2011.

[50] S. Agrawal, R. Roman, M. L. Das, A. Mathuria, J. Lopez, "A novel key update protocol in mobile sensor networks", *Proc. 8th Int. Conf. ICISS*, Vol. 7671, pp. 194–207,2012.

 ©IJSRED:All Rights are Reserved