ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Security Analysis of Encrypted Key Exchange With Diffie Hellman In Wireless Sensor Networks

Deepa Devarajan
deepa.11601746@gmail.com
Department of computer science
Lovely Professional University

Gursharan Singh
gursharan.16967@lpu.co.in
Department of computer science
Lovely Professional University

Dr. Pooja Gupta
pooja.19580@lpu.co.in
Department of computer science
Lovely Professional University

***Abstract*—This paper gives a brief introduction to the concept of Wireless Sensor Networks, an evolving technology. The applications of WSNs vary from day to day operations to critical applications like in the military. It further discusses certain security issues in WSNs and proceeds to a detailed analysis of the Diffie Hellman Encrypted Key Exchange (DH-EKE) and its consumption of energy when applied in Wireless Sensor Networks.**

Keywords—Wireless Sensor Networks, Eavesdropping, Denial of Service, Sensor Node Compromise, Diffie Hellman Encrypted Key exchange

I. INTRODUCTION

Wireless Sensor Networks is an emerging technology, and with its ever-growing demand, there comes several security issues as well. Wireless Sensor Networks employs miniature devices known as sensor nodes which allow easy setup and flexible network layout. Sensor nodes are tiny devices which, due to their immense versatility, have found use in various fields. These sensor nodes have high sensing capabilities, informational processing, logical decision making, and synchronization with other sensor nodes for fast message transmission leads to their immense utilization in highly confidential as well as sensitive applications in various branches like Health Analysis (Body Area Networks), ecology, armed forces as well as commercial applications. Due to their extensive usage in different fields, these sensor nodes must possess capabilities such as acting as an independent processing unit, detecting the neighbor nodes, architecting routes to their destinations, each of the sensor node, thus contributing towards the development of a connected as well as feasible, sustainable Wireless Sensor Network. Considering the applications of the sensor nodes, security is the buzzword. Ensuring security in sensor nodes (wireless sensor networks) is of chief importance and an alarming issue.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

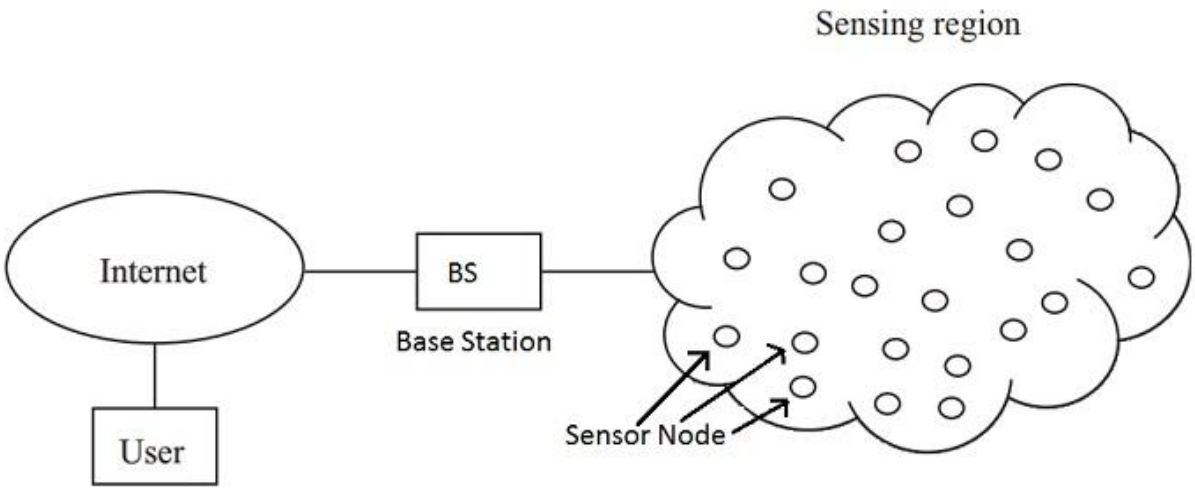


Figure 1: Generic structure of Wireless Sensor Network

Security issues include eavesdropping, denial of service attack, sensor node compromise and many more. In general, the security in wireless sensor networks can be categorized into two classes - (i) content security and (ii) context security. Content security refers to coming up with security mechanisms to ensure the integrity of the data transmitted though the network. Context security refers to protecting the contextual information related with a Wireless Sensor Network, such as the sensor node's location, which is encrypting the data renders the location of occurrence of the event. We have several alternatives to mitigate the known attacks, However, the attacks which are not known, are a threat to the wireless sensor networks. Hence, we need an attack prevention mechanism that can protect the wireless sensor networks from unknown, potential attacks. The current defense approaches are detection-approach, like enforcement of the Intrusion detection Systems and the preventive-approach such as implementing access controls.

II. LITERATURE REVIEW

Yong Wang et al. [2006] Presents a list of Wireless Sensor Networks (WSNs) relevant security concerns. Next, with their comparable countermeasures in WSNs going on to offer a holistic approach of security issues, they detail the weaknesses, safety requests, and attacks. Security concerns are divided into five groups: key management, authentication, secure collection of data, safe routing, and identification of intrusion. Along the way, they highlight the benefits and drawbacks of several WSN security protocols and further compare and assesses these protocols based on each of these five classes. They also emphasize on the open research problems in each subfield and concludes with potential research directions on security in WSNs.[1]

Ivana Tomic` et al. [2017] Deepen the chief security techniques and their impact on the most prominent protocols and standards such as IEEE 802.15.4, s, routing protocol for low-power and loss network routing (RPL), IPv6 over low-power wireless personal area network and restricted application, Berkeley media access control for low-power sensor networks, backpressure collection protocol, Set tree protocol, routing protocol for low-power and loss network (LPN) routing protocol, and restricted application protocol used in WSN implementations, where potential security risks and current countermeasures are addressed on each WSN stack level. This article culminates in a deeper analysis of layer 2, i.e. attacks on the network layer based on the routing protocol of the RPL. Using the network simulator-Cooja, it quantifies the effect of targeted attacks on network performance. Eventually, the paper addresses new

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

network layer security research opportunities and how to use Cooja as a template for developing new WSN systems safeguards.[2]

Jun Wu et al. [2016] Introduced a hierarchical structure focused on the chance exploration and use control (UCON) technologies to boost WSN security while taking into account WSN's minimal-complexity and high-security requirements. In addition, to classify unidentified attacks, they use a complex adaptive chance discovery method. A unified architecture is developed in which low-level discovery of attacks with simple laws is incorporated in sensors and high-level detection of attacks with complicated rules is carried out in sinks and at the base station to model and execute a process using the method above. In addition, network virtualization feature and software-defined networking techniques are used when defining both low-level and high-level breaches to achieve attack alleviation. An study to acquire an assault data set for evaluation was conducted. A experiment was then intended to calculate the use of the resource and the rate of identifying attack. The results show the viability and efficacy of the suggested scheme.[3]

Yanjiang Yang et al. [2010] Proposed a heterogeneous architecture for WSNs to expedite security enforcement, wherein a wireless sensor network is segregated into clusters, each cluster possessing a high-end head, also known as a cluster head. Furthermore, the cluster heads are furnished with trusted computing technology (TC), so that they serve as trusted parties online, thereby anticipated to assist in enforcing security efficiently.[4]

Xiangqian Chen et al. [2009] Identify the threats and loopholes in WSNs and review the defense systems based on the networking layer protocol analysis and also provide an overview of the various security issues. Firstly, this paper identifies the threats and loopholes in WSNs and review the defense systems based on the networking layer protocol analysis. Later on, it moves on to it, providing an overview of security concerns. These issues are classified into seven divisions: Key managing, cryptography detection through blocking, safe location protection, a secure fusion of records, secure routing, as well as other security issues. The benefits and disadvantages of modern security along with the other security systems in each category are scrutinized. Additionally, it also summarizes the procedures and approaches used in these divisions and highlights the open research issues and inclinations in each area.[5]

Thaier Hayajneh et al. [2013][6] Proposed a new protocol for the choice of energy and safety routes (ESARS) for WSNs. ESARS protocol's first segment selects a path that optimizes the life span of the network based on a single measure. Depending on the route's estimated safety hazard, the next segment defines the optimal protection rate for the chosen path. The two pieces are mentioned separately in the books generically, and this paper centralizes the two sections into one protocol. Utilizing rational analysis and extensive simulations, the suggested protocol is evaluated and correlated with various protocols. The results demonstrate that the protocol not only fulfills its central purpose of raising the lifespan of the network by significantly reducing the sensor death rate, but also employs the most efficient safety feature for the chosen path. In addition, specific threshold parameters have been introduced in ESARS to allow functionality according to the application specifications in which sensors are used.

Kashif Kifayat et al. [2012] proposed a [7] unique component-based security system (COMSEC) based on reactive and proactive components to enhance Quality Of Service in WSNs - wireless sensor networks. Each element, aggregated with the other, takes care of a specific security issue. The recommended system provides better as well as guarded communication, detects Sybil attacks, secure data collection and safeguards against replication, node capture attacks. The component-based security system has been assessed and weighed against the prevalent schemes. The results reveal a notable enhancement in resistance abreast node capture attacks, privacy, connectivity, memory overhead and Sybil attack discovery data confidentiality.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Daojing He et al. [2013] classify the security vulnerabilities of several protocols used to ensure security in wireless sensor networks and analyze a recently suggested explication addressing this problem. Furthermore, they recommend an improvement to this solution to make the safety functionality more effective.[8]

Di Ma et al. [2010] review the security issues in some current and surfacing classes of wireless networks and try to identify objectives for prospective research. In studying relevant works, they seek to classify modern security challenges and shortcomings of comprehensive strategies. Specific problems arise from the untended, intermittently correlated, and perhaps mobile network performance. Consequently, we need to foresee perils emanating from malicious exploitation of such network peculiarities and devise relevant security preventive measures. Moreover, since certain developing wireless networks are ad hoc in nature, infrastructure-independent privacy and security methods are especially fitting. Conclusively, developing wireless devices like the R-Sensors stimulate the advancement of modern cryptographic primitives and protocols.[9]

III. SECURITY ISSUES IN WIRELESS SENSOR NETWORKS

Security issues include eavesdropping, denial of service attack, sensor node compromise and many more. In general, the security in wireless sensor networks can be categorized into two classes - (i) content security and (ii) context security. Content security, as the name suggests, refers to securing the content i.e., data transmitted through the wireless sensor networks. This includes protecting the data from being tampered by any means. Context security refers to protecting the contextual information related with a Wireless Sensor Network, by ensuring confidentiality such as the location of the sensor node which is encrypting the data renders the location of occurrence of the event. We have several alternatives to mitigate the known attacks, However, the attacks which are not known, are a threat to the wireless sensor networks. Hence, we need an attack prevention mechanism that can protect the wireless sensor networks from unknown, potential attacks. The current defense approaches are detection-approach, like enforcement of the Intrusion detection Systems and the preventive-approach such as implementing access controls.

A. Sensor Node Compromise

As communication in wireless sensor networks is established sensor nodes in the network, each node is a potential target for an adversary. As these nodes are geographically dispersed, it is not feasible to individually look over each node and shield it from attacks. Spoofing is a possible attack in such a scenario, wherein the attacker creates a malicious sensor node which impersonates as a legitimate node in the network. Once the attacker gains access to the network several attacks such as data falsification, unauthorized access and extraction of confidential data from network readings, and denial of service can be mounted.

B. Eavesdropping

Eavesdropping is a scenario wherein an adversary gets hold of private data by continuous analysis among nodes. ring transmissions between nodes. Encrypting sensor node transmission data is a solution to eavesdropping. However, it also gives rise to yet another issue, which is, key exchange. This issue is further discussed in detail.

C. Denial of Service (DoS) Attacks

DoS attack is a kind of attack in which the attacker, instead of gaining illegitimate access and/or modifying data, floods the server with malicious requests greater than the server bandwidth, due to which the server is unable to process legitimate requests, consequently disrupting network functionality. These attacks can be exercised either at the physical layer, i.e., via radio jamming or by injecting

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

malicious transmissions to intervene with sensor network protocols or damage the central nodes. Attackers may also try to cause battery exhaustion of sensor nodes by sending a constant series of useless communications processing which the targeted nodes will disburse energy and may also forward to other nodes.

IV. DIFFIE HELLMAN KEY EXCHANGE

Diffie Hellman Key exchange is an efficient as well as secure mechanism for key exchange. This is used for providing the features of authentication as well as confidentiality while communication between nodes in a network. Diffie Hellman Key exchange can be exercised in public key cryptography, for ensuring secure distribution of keys between sender as well as receiver. As the figure 2 depicts, there are two entities, say, Alice and Bob. Each entity contains a pair of keys- one public and one private. Next step involves exchange of the public keys of the two entities. Each entity then creates a key with the use of their private key and the public key of the other. Mathematically, the two keys derived are found to be equal. In a wireless sensor network, communication occurs between two nodes at a time. If a network has n nodes, each node must possess (n-1) keys to communicate with the other (n-1) nodes, summing up to an overall of n(n-1) keys in the network.

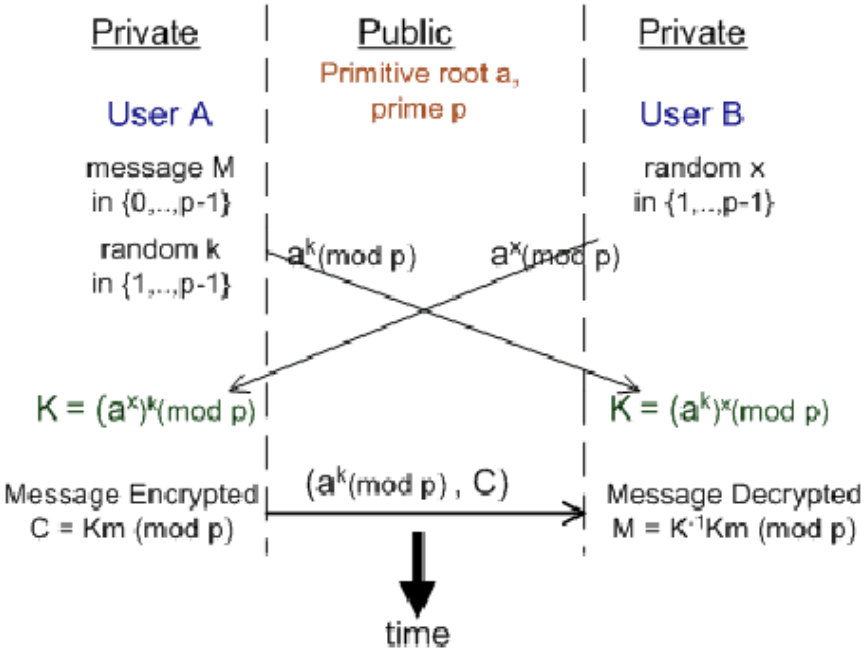


Figure 2: Diffie Hellman Key exchange process

A. Diffie Hellman in Wireless Sensor Networks

The Diffie Hellman Key Exchange uses exponential & logarithmic functions. Firstly, all the nodes in a network agree upon a constant prime- p and the base g. A node N1 will then select a private key xp and will generate a public key xpub using the formula-p^{xp} (mod g). similarly, another node N2 chooses a private key yp and generates a public key ypub=p^{yp} (mod g). For communication to happen between N1 and N2, the two must exchange their public keys i.e., xpub and ypub. N1 generates another secret key kxy=$ypub^{xp}$ (mod g) and N2 generates kyx= $xpub^{yp}$ (mod g). As the power function is symmetric, it turns out that kxy=kyx. And this common key acts as the generic session key during communication between the two nodes.

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

V. DIFFIE HELLMAN ENCRYPTED KEY EXCHANGE's ENERGY CONSUMPTION

Due to the criticality of applications in which Wireless Sensor Networks are used, the sensor node readings must be confidential and must not be available to an attacker. Hence, efficient schemes are required to ensure security in WSNs. DH-EKE employs a weak password to authenticate the public key exchange which are used to retrieve session keys.

The figure below depicts DH-EKE key agreement throughout all nodes in wireless sensor network. It occurs in a three-phased key agreement approach:

- Phase 1: This phase involves setting up of initial pre-established parameters as well as keys among all the nodes in the network.
- Phase 2: This stage is the main step of exchange where each pair of neighboring sensors shares partial keys.
- Phase 3: This is the phase wherein each node pair calculate their shared secret key.

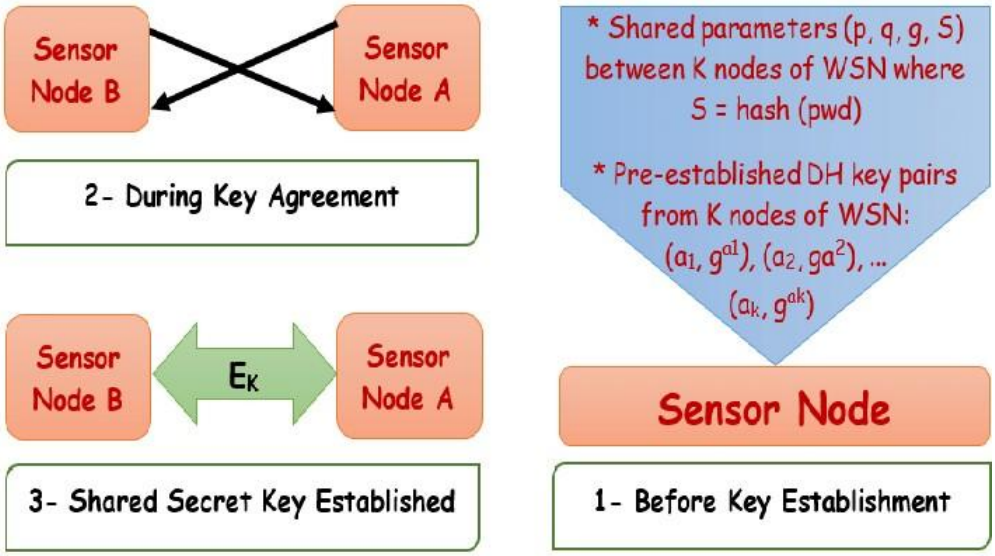


Figure 3: EKE key agreement across all nodes

The energy dissipation in a Wireless Sensor Network can be determined by individually assessing the components of a WSN that consume the most energy. In a sensor node, the prime energy consumers include the sensing device, transceiver as well as the microprocessor. However, when packets are transmitted and received, energy is frittered in a high amount.

Energy consumption on applying Diffie Hellman Encrypted Exchange in Wireless Sensor Networks can be calculated by computing the total energy consumed by each sensor node, this includes dissipated energy when a number of bits are received or transmitted over a particular distance. Thus, the number of bits transmitted/received via a node with respect to Diffie Hellman Encrypted Key exchange is:

(M + W) x bits/Message → Total number of communication bits
M is number of messages transferred and W is number of messages received

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Diffie-Hellman Key Exchange

Step	Alice	Bob
1	Parameters: p, g	
2	$A = \text{random}()$ $a = g^A \pmod p$	$\text{random}() = B$ $g^B \pmod p = b$
3	$a \longrightarrow$ $\longleftarrow b$	
4	$K = g^{BA} \pmod p = b^A \pmod p$	$a^B \pmod p = g^{AB} \pmod p = K$
5	$\longleftarrow E_K(data) \longrightarrow$	

Figure 4: Diffie Hellman Encrypted Key Exchange

As per Figure 4, M+W=6, which means that, to establish the common secret key, every two adjacent nodes are passing six messages. Therefore, total energy consumption Etotal = ER + ET. Let's assume the transferred packets have a bit size k, same as that of the shared key (Ek), then ET can be computed as:

ETotal = K x 6 × (ER + ET) nJ, …. (1)

where:

ET = Eelec + Eamp × Distance2 and ER = Eelec for 1-bit.

If Berkeley nodes are used with (TElec = RElec = 50.0 n J / bit
and
TAmp= 100 p.0 J / bit/ m2)
then:
ETotal = 6K × N × (100 + 0.1×D2)) * 10 - 3 μ J …. (2)
where:

K is the size of the key shared in DH-EKE.

N is shared parameters with number of neighbor nodes with.
Sensor node and neighbor node's distance is D.

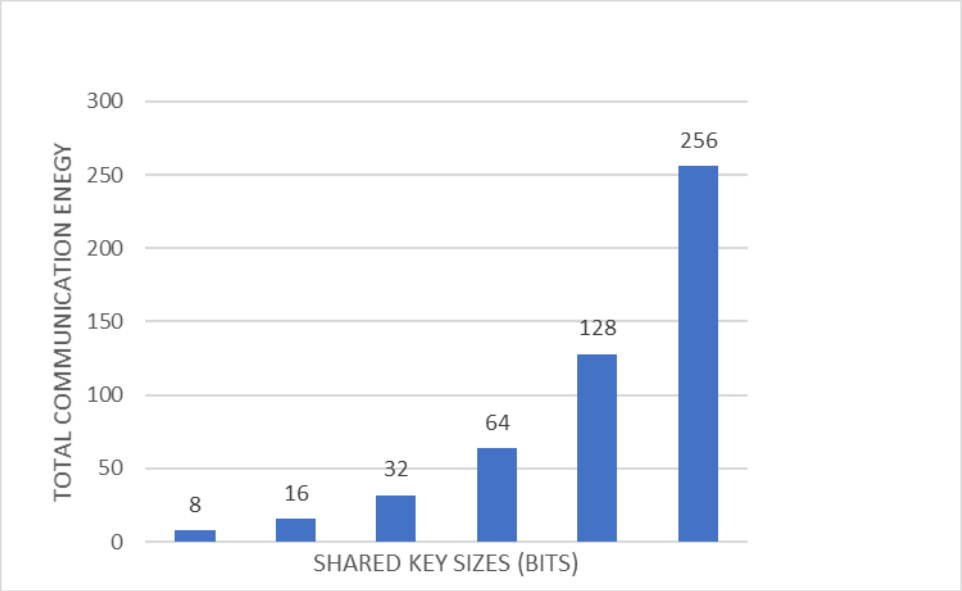


Figure 5: Relationship between bit length and energy consumption

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Figure 5, Indicates the connection between power consumption during interaction and the shared key size bit length whenever the distance from the neighboring node is fixed (distance = 1 m). The figure evidently portrays that the DH-EKE bit length is directly proportional to the energy consumed.

Figure 6, depicts a graphical yet three-dimensional representation of how the energy consumption varies with the number of neighbour nodes for different bit key lengths. For 256-bit DH-EKE, the maximum energy parameter was reported with 10 neighbors having pre-equipped parameter with approximately 1.54mj. Ultimately, the contact gap was determined to be set because it does not contribute significantly to the equation for energy consumption., in which it is multiplied by 0.1nj, a small scalar value.

A completely connected WSN containing R sensor nodes with K-bit DH-EKE key would have an energy consumption of:

$$Ewsn = 6*\sum^{R} n=1 (K*N*(100 + 0.1*D\hat{}2) *10\hat{}-9) J$$

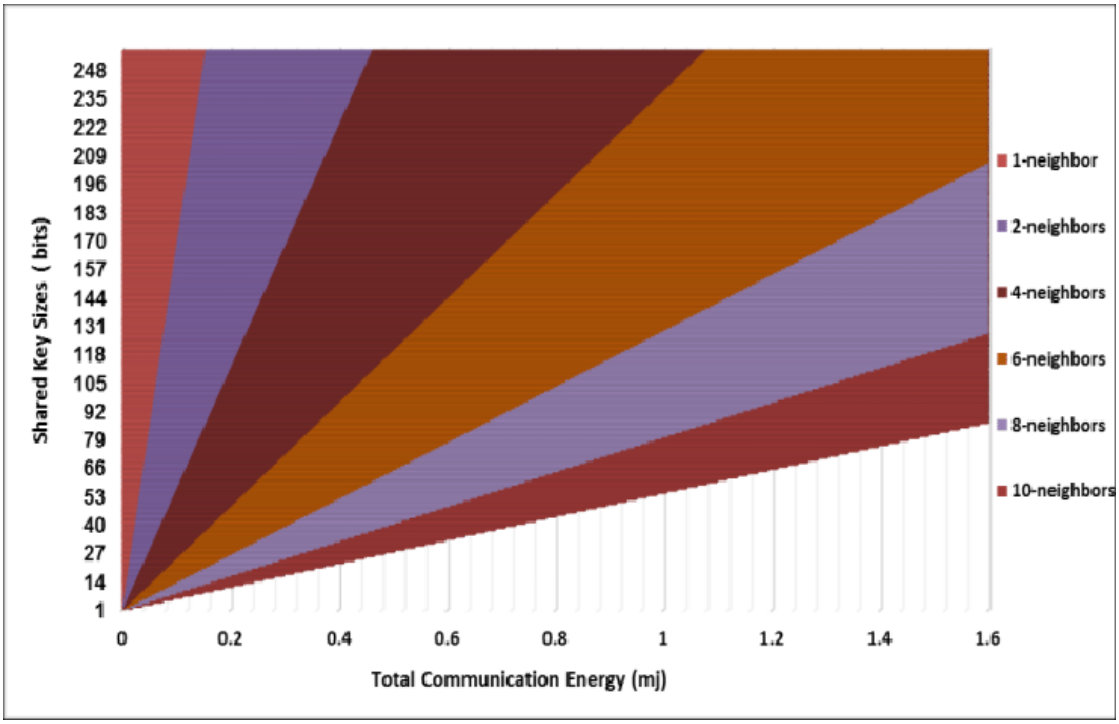


Figure 6: Energy consumption Vs. Bit length for different neighbors over fixed communication distance of 1m.

Taking
R is 100, D is1m, N is equlas 3 neighbours and K is 64-bit, Etotal = 11.42mj.

VI. CONCLUSION

This paper, along with a deeper analysis of the "Diffie Hellman Encrypted Key Exchange", addresses several security problems related to Wireless Sensor Networks. The energy usage of applying DH-EKE in homogenous WSNs holding the contact distance constant and varying the number of neighboring nodes revealed that the energy consumption depends on key length, sensor node features as well as the number of neighboring nodes.

REFERENCES

Copyright © 2019Authors

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[1] D, chan & guizani, m. (2014). Small data dissemination for wireless sensor networks: the security aspect. IEEE wireless communications, 21(3), 110–116. Https://doi.org/10.1109/mwc.2014.6845055

[2] Tomic, & mccann, j. A. (2017). A survey of potential security issues in existing wireless sensor network protocols. IEEE internet of things journal, 4(6), 1910–1923. Https://doi.org/10.1109/jiot.2017.2749883

[3] Chen, x., makki, k., yen, k., & pissinou, n. (2009). Sensor network security: a survey. Ieee communications surveys and
tutorials, 11(2), 52–73. https://doi.org/10.1109/surv.2009.090205

[4] Wu, j., ota, k., dong, m., & li, c. (2016). A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities. IEEE access, 4, 416–424. https://doi.org/10.1109/access.2016.2517321

[5] Hari, p. B., & singh, s. N. (2016). Security issues in wireless sensor networks: current research and challenges. Proceedings - 2016 international conference on advances in computing, communication and automation, icacca 2016. Https://doi.org/10.1109/icacca.2016.7578876

[6] Ullah khan, h., & knoll, w. (2016). Dna diagnostics: optical or by electronics? International journal of sensor networks and data communications, 01(s1), 1–3. Https://doi.org/10.4172/2090-4886.s1-001

[7] Habib, s. M., ries, s., & max, m. (2010). Towards a trust management system for cloud computing market places: using caiq as a trust information source. Security and communication networks, (november 2013), 1–18. Https://doi.org/10.1002/sec

[8] Kashif kifayat, madjid merabti (2013). Component based security system(comsec) with qos for wireless sensor networks. Security and communication networks, (November 2012), 1–18. Https://doi.org/10.1002/sec

[10] Yanjiang yang, jianying zhou (2010). Better security enforcement in trusted computing enabled heterogenous wireless sensor networks: security and communication networks, (january 2010), 1–18. https://doi.org/10.1002/se

Copyright © 2019Authors