ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

# Channel Based Key Generation with Q-S Composite Technique in Wireless Sensor Networks

Harisha P Haridas[1], Raseena Yousuf[2]

*M.Tech Student[1], Assistant professor[2]*

*M Tech Communication, ECE Department, A P J Abdul Kalam Technological University*

*APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY*

[1]harishaharidas@gmail.com

[2]raseen.yousuf@gmail.com

***Abstract*— Network security defines the protection of a mobile network, and its services from unauthorized modifications, destructions or disclosures from the environment. Symmetric encryption is commonly used by wireless sensor networks inorder to provide security. Random key predistribution is the effective key distribution technique that is used by majority of symmetric encryption system. Channel plays an important role in WSN, and based on the channel some attacks may introduced inside the network, which is also emphasized in this paper. Considering the challenges in conventional methods, a promising protocol called channel based key generation with Q-S Composite technique is proposed here to distribute secret key to legitimate users. In this approach, the organization of secret key material allows a strong reduction by exploiting the channel variations to extract a common encryption key at both sides of link, and by the limited number of predistributed keys used in channel based key generation. An eavesdropper, however do not share the physical channel between two legitimate users and cannot extract any information, since the data series on both sides are highly correlated values. The simulation results shows that, our proposed scheme can provide efficient memory managing with very high level of security against eavesdropping.**

***Index Terms*- Key management, WSN, symmetric encryption, random predistribution.**

## I. INTRODUCTION

Wireless sensor networks are becoming more and more popular service, that are utilized in many industrial and commercial applications, because of its technical advancement in processor, communication and usage of low power devices. Sensor nodes are capable of sensing the environment and performing many real time applications like, neighbor node discovery, smart sensing, data storage and processing, data aggregation, target tracking, control and monitoring, node localization, synchronization efficient routing between nodes[1]. Each node is capable to perform data gathering, sensing, processing and communicating with other nodes. Because of its limited resource, limited memory, limited computation and limited power sever security problems may arise.

Although, the sensor devices are inadequate in their energy, computation and communication capabilities. When sensor nodes are deployed in hostile environment, security becomes extremely important as they are prone to different malicious attacks. For example, an adversary can easily listen to the traffic, impersonate one of the network nodes or intentionally provide misleading information to other nodes.To ensure the services in WSN cryptographic [2] mechanisms like symmetric and asymmetric methods are proposed. To achieve security in WSN, it is important to be able to encrypt and authenticate message send between sensor nodes. This is a mathematical tool connected to the aspects of information security such as, confidentiality, data integrity, entity authentication and data origin authentication.

Symmetric cryptosystem [3] is most commonly used in WSN, in which same key is used for both encryption and decryption. The key is kept secret between source and sink. The organization of these symmetric key is known as key distribution. Since sensor nodes are low computational devices with less memory, the requirement of more efficient key distribution scheme in terms of memory and computational, communication complexities without compromising the level of security is necessary.

Two basic symmetric distribution schemes used for WSN are, PGK(Plain Global Key) [2],[3]scheme and FPWK (Full Pairwise Key)scheme. In both approaches the nodes do not execute any additional operation for key establishment, since all keys are predistributed before deployment. Also, do not

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

require knowledge and do not implicate any computational or communication overhead. PGK involves limited memory overhead, since here, a unique key is used by all the nodes in the network. However, in FPWK, each node shares a specific key with each other nodes in the network and so, this can provide better security than PGK. Also, in PGK, any opponent that capture the secret key will able to eavesdrop on any link and produce more compromised nodes. Likewise in FPWK, it consumes large memory area for key management, because here, each node need to share number of keys equal to the quantity of nodes in the network.

All the key pre-distribution [4] techniques can be divided in tomethods, which are: probabilistic, deterministic and Hybrid. In the probabilistic methods keys are chosen on the random basis and then placed into the sensornodes.In the deterministic method some patterns are used to select the keys from the large pool. Finally, the hybrid technique uses both the deterministic and hybrid method to select the keys.The random key predistribution scheme also known as basic scheme. In this approach, a large pool of keys is created, from this pool a ring of keys are randomly chosen andstored in every sensor node. Any two nodes which find common keys can use these shared keyfor secure communication.

One of the important key distribution scheme based on random key predistribution is the q-s-composite [5] scheme. Here, any two neighbouring nodes can establish a link only if they share at least q keys. And also, QSC is given by a parameter s, which represents the maximum quantity of starting keysused for a pairwise key establishment. For the generation of pairwise key, the two nodes performs bit wise XOR operation on all shared starting keys.

In this paper, a comparative analysis demonstrates that the proposed approach ie channel based key generation with q-s composite technique for WSN, provides a higher level of security and performance than the existing random key predistribution schemes by considering the effect of channel attacks. Although q-s composite scheme is flexible, efficient and simple to employ, provide good scalability with efficient memory managing, it did not consider the fact that, channel plays an important factor in WSN and based on channel some attackers can include inside network. Sensor networks are deployed in conditions where the wireless communication channel varies dramatically due to fading and shadowing, which is considered a disadvantage for communication. Interestingly, these channel variations can be employed to extract a common encryption key at both sides of the link and that what we done in this current paper.Legitimate users share a unique physical channel and the variations thereof provide data series on both sides of the link, with highly correlated values. An eavesdropper, however, does not share this physical channel and cannot extract the same information when intercepting the signals. So,here implementing channel-based key generation for q-s composite scheme which can be done in any realistic practical conditions. Here, employing a process known as key reconciliation and error free keys are generated. The key-generation system is computationally simple and therefore compatible with the low-power devices and low-data rate transmissions that is commonly used in wireless sensor networks.

The remainder part of this paper is organized as:In section II we briefly described the related works. In section III we present the proposedq-s composite with channel based key generation technique for WSN scheme, while in section IV we extensively evaluate the performance of channel-based key generation by comparison with the existing q-s composite scheme. Finally, in section V, we conclude the paper.

## II. RELATED WORKS

In [6], Eschenauer and Gligor proposed a basic scheme for random key predistribution in which, a random pool of keys p picks out of the totalpossible key space. For each node, r keys are randomly selectedfrom the key pool p and stored into the node's memory.This set of r keys is called the node's *key ring*. Thenumber of keys in the key pool, p is chosen such that two
random subsets of size r in p will share at least one keywith some probability. During thenetwork initialization, each node checks if there are sharedkeys with other neighbouring nodes. Although, this scheme require less quantity of memory, due to lower level of security, this cannot be used in environments demanding highest security

The variation to this basic scheme is the Q-Composite Random Key Predistribution Scheme [5], where q common keys are needed to establish the secure link between nodes. That is here, two nodes have to share at least q starting keys to establish a link. They generate a pairwise key by performing a hash function on the concatenation of all shared starting keys. In this scheme the numbers of keys overlap increased, so it is difficult for an adversary to break down the communication link. The q-composite keys scheme offers greater resilience against node capture when the number of nodes captured is small. But, it require large memory area for key management.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

In order to address these issue, another protocol called q-s-composite is proposed in [7]. The main novelty of this scheme is that the quantity of starting keys used for the generation of a pairwise key is limited by an upper bound (called s). Instead of generating a pairwise key per neighbouring node, each node stores the information for the key generation and computes the pairwise key when it is required by the security system of the network. Here bit-wise XOR operation is introduced for pairwise key generation. The main advantage of q-s-composite is represented by an efficient memory management, which allows to store a larger quantity of keys and consequently it can improve the resilience of the protocol. But this approach did not consider the fact that, the channel plays an important factor in WSN and based on channel some attackers can include inside network.

Key generation using temporally and specially correlated channel coefficients is described in [8]. Here secret key establishment is performed establishing secret keys using the common wireless channel, withparticular emphasis on the spatial and temporal correlations of the channel coefficients. Also investigate the influence ofchannel correlation on the bound of the key size generated from the common channel using a simple single-input single-output channelmodel. Here the development of a practical key generation protocol is based on a published channel coefficient quantizationmethod and incorporating flexible quantization levels, transmission of the correlation eigenvector matrix, and LDPC coding to improvekey agreement in an authenticated public channel. This paper proposed quantization of the uncorrelated channel samples usingflexible quantization levels and error correction using LDPCcodes to enhance key agreement over an authenticatedpublic channel.

Another scheme for effective secret key generation is by using wireless signal strength [9]. In this paper real world measurements of RSS (Received Signal Strength) in a variety of environments and settings is proposed. And here developed an environment adaptive secret keygeneration scheme that uses an adaptive lossy quantizer in conjunction with Cascade-based information reconciliation and privacyamplification. This approach performs the best in terms of generating high entropy bits at a high bit rate.The conclusions drawn in this paper, specifically thepredictable channel attack, are primarily for key extractionusing RSS measurements, and these may not directly applyto key extraction using channel impulse response measurements.

## III. PROPOSED APPROACH

Most of the wireless sensor networks are deployed in conditions where the wirelesscommunication channel varies dramatically due to fading and shadowing, which is considereda disadvantage for communication. We can use these channel variations can be employed toextract a common encryption key at both sides of the link. Legitimate users share a unique physicalchannel and the variations thereof provide data series on both sides of the link, with highlycorrelated values. An eavesdropper, however, does not share this physical channel and cannot extractthe same information when intercepting the signals.

The parameters of C_QSC are configured before the networkdeployment, which are:

- n- the quantity of nodes in the network
- p- the quantity of starting keys in the pool
- r-the quantity of starting keys in each ring
- q-the minimum quantity of shared starting keys required to establish a linking nodes per node, v is constant.

In C_QSC, like in previous schemes based on random key distribution [9], a ring of r starting keys is randomlypicked up per each node from a pull of p starting keys. Like in QSC, here also any two neighbouring nodes can establishalink only if they share at least q keys. And here the parameter s,which represents the maximum quantity of starting keysused for channel establishment.

Here, the wireless sensor nodes in this paper employ communication according to the IEEE802.15.4standard, of which the MAC (Media Access Control) layer includes AES128 (Advanced EncryptionStandard) with seven security levels, of which the highest level combines 128 bits AES encryption and128 bits MIC (Message Integrity Code).However, key management and generation algorithms are notincluded and should be provided by the upper network layer. It is exactly the key distribution that ischallenging and current techniques are often based on the predistribution of secret material, causinglarge memory overhead and security issues.So this paper proposes a channel-based key generation scheme in which the nodes are modified to exchange packets between legitimate parties within a very narrow time slot, allowing theaccurate estimation of the channel at both ends of the link. The raw Key Error Rate (KER) is determinedand a threshold is employed to reduce the KER below a level for which further reconciliation yieldserror free keys [8].Keys generated following this approach can be constantly updatedand hence should be virtually impossible to break, provided that careful hardware construction ofthe sensor node makes side-channel attacks (by

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

measuring other electrical parameters such as powersupply current) impossible [10].

Throughout the paper, the letters A, B and E will be used. A and B are the legitimately communicating nodes, simultaneously moving around, whereas E is the stationary eavesdropping node, trying to assessthe keys used by A and B. In the processing of channel measurements, first the transceiver chip in node performs channel measurements by means of an analog logarithmic detector,which are further sampled as 8-bit values, directly expressed in dBs. The resolution of the measurementis 1 dB, according to the datasheet. Inaccuracy can result from channel variation, node-to-node parameterspread, or system imbalances such as differing antenna performance and matching. Hence, the bytesthat result from the reciprocal detectors are generally not equal, despite their high correlation.

To design a system that functions in practice by exploiting these channel measurements,a quantizer is applied at node A side to extract only one bit per channel measurement accordingto the following procedure:

- Determine the moving average of the last seven RSS values (corresponding to the average over the last 7 s) [11].
- If the current RSS value crosses a threshold of N dB above or below this value, a 1 or a 0 bit is generated, respectively.
- B is informed about the generation of a key bit via the wireless channel, without revealing the actual value of the bit.
- If the threshold is not crossed, no bit is generated.

The quantizer at node B side also extracts one bit per channel measurement, as follows:

- Determine the moving average of the last seven RSS values
- If B is informed by node A that it has generated a key bit, node Balso generates a key bit:1-bit is generated if node B measured RSS value is above the threshold or 0-bit is generated otherwise.

If node A generates the master key, she will choose and apply the threshold level. Each time node Auses an RSS value to generate a key bit, she will immediately inform node B over the wireless link.The information of course does not contain the actual value of node A's key bit. Node B can now generate its own version of the key bit, based on its own RSS measurement. This approach [9] is absolutelynecessary in order for node A and node B to use sets of RSS values that are sampled in correspondingtime slots.Independently choosing RSS samples on both ends of the link via equal thresholds does not workin practice. Due to the imperfect reciprocity of the measurements, the generated keys would quicklyrun out of synchronization since, at some time instances, only one party would generate a key bit.

Only one RSS measurement per second is presented to the quantizer, in order to obtain subsequentrandom bits that are sufficiently decorrelated. The time interval of one second corresponds well to therate of change of the RSS values recorded for normal moving speeds of about 0.5 m/s. The faster moving speeds could allow faster key generation, but, at the moment, the rate of which the RSS values arepresented to the quantizer is kept fixed. Employing higher thresholds further limits the key generationrate because more measurements are dropped. However, higher thresholds will result in bettermatching between bilateral raw keys.The bilateral set of raw keys needs further reconciliation to exactly match. The (11, 7)-Hammingforward error correcting code is employed to achieve equal keys. After pseudo-random bit interleaving, node A's raw key is taken as the master key and subdivided into 11-bit groups. For each group,four Hamming check bits are calculated and transmitted to Bob. The potential key errors in B's keyare corrected based on the check bits from node A's key. As a last step, de-interleaving is performedto undo the interleaving. Interleaving scrambles bits in pseudo-random order to spread groups ofsubsequent key errors over a large number of Hamming words, improving the performance of theerror correcting code.Transmitting the check bits reveals some information about the key to a potential eavesdropper,assuming the unlikely fact that the eavesdropper has all detailed information about the completekey-generating system. Employing the Hamming code and revealing four check bits, results in 27 valid11-bit words. The effective key length is hence reduced by a factor 7/11 if the eavesdropper performsa brute-force attack with knowledge of the check bits. However, even then, a sufficiently long andregularly updated key cannot be reconstructed by an eavesdropper.

## IV. PERFORMANCE EVALUATION

This section evaluate the performance of C-QSC scheme with the existing QSC scheme.

### *A. Control Overhead*

Network control mechanisms are used to regulate the flow of traffic and ensure effective data transport in communication networks. Typically, network control actions are taken in response to changes in the network state. Therefore, network control tasks

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

necessitate the exchange of information regarding the network state, which we refer to as control information or protocol information. Examples of such control information include source and destination addresses, CTS/RTS messages, channel state information (CSI), and packet loss rates. These

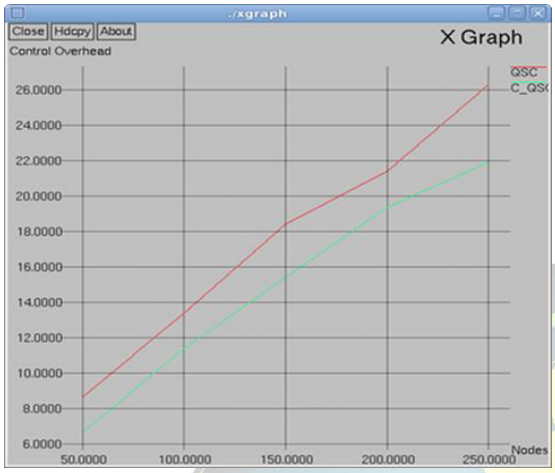



Fig 1: Control overhead versus number of nodes in C_QSC & QSC

signals directly impacts network performance, and often leads to significant overheads. And, there is a tradeoff in the amount of control information sent to the controller (as overhead) and the performance of the network control mechanism. This applies to a wide range of network control problems, such as opportunistic scheduling, congestion-based flow control, and link state routing and back pressure routing. Fig 1, shows the control overhead required for C_QSC and QSC with increase in number of nodes. By analyzing the graph it is clear that,QSC cause more control overhead.

### B. *Average Throughput*

Throughput is the maximum rate of production or the maximum rate at which something can be processed. When used in the context of communication networks, throughput or network throughput is the rate of successful message delivery over a communication channel. The data these messages belong to may be delivered over a physical or logical link, or it can pass through a certain network node. Throughput is usually measured in bits per second.Channel utilization is instead a term related to the use of the channel disregarding the throughput. It counts not only with the data bits but also with the overhead that makes use of the channel., the throughput would not be only associated to the nature (efficiency) of the protocol but also to retransmissions resultant from quality of the channel. Fig 2 shows the variation of average throughput according as increase in number of node. This implies that the average throughput obtained for C_QSC is high compared to QSC and proportional increases as the number of nodes increases.

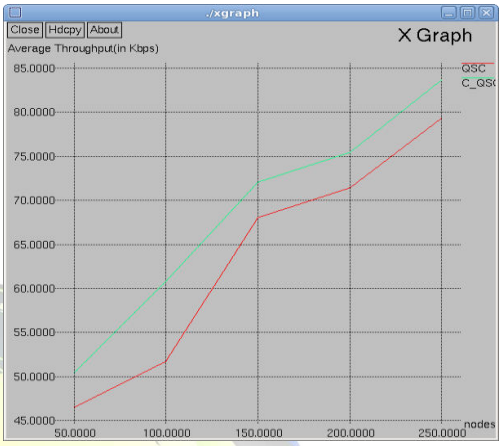
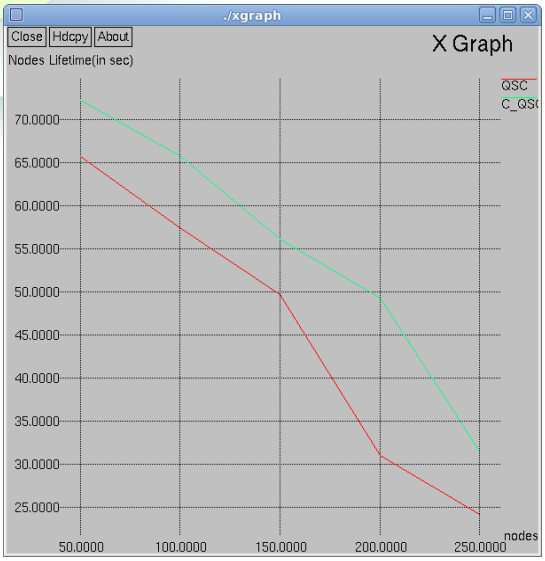



Fig 2: Average throughput versus number of nodes in C_QSC & QSC

### C. *Node Lifetime*

Node lifetime is a key performance metric in wire-lesssensor network (WSN) research. Simplistic assumptionsand novel lifetime estimation techniques invariably prove to be extremely unreliable in practice. Each node in thesensor network community agrees that sensor node lifetimeis a key metric, preliminary studies both in simulation andon real hardware use calculations based on datasheet forthe expected network lifetime. The simulation result shows that C_QSC scheme can achieve better node lifetime than QSC, which shown in fig 3.



ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Fig 3: Node Lifetime versus number of nodes in C_QSC & QSC

### D. Energy Consumption

Energy consumption is one of the most important metrics in wireless sensor networks because of the limited power supply in sensor nodes.Many efforts have been taken to reduce the energy consumption of the hardware, software, communication protocols and applications.

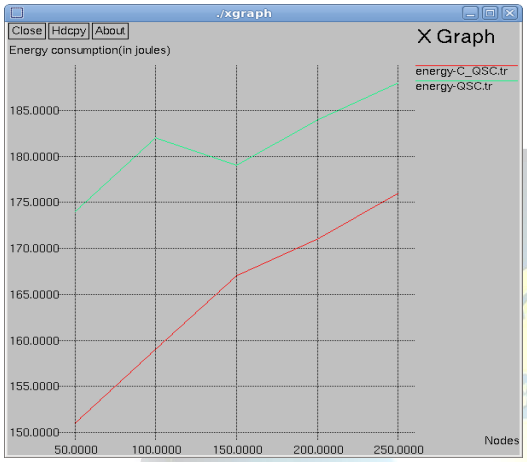



Fig 4: Energy Consumption versus number of nodes in C_QSC & QSC

The requirements of small size and low cost result in limited energy supply on sensor nodes, so energy consumption is one of the most important metrics in WSNs. In order to extend the lifetime of sensor networks, many efforts have been taken to reduce the energy consumptions of the hardware, software, communication protocols and applications. Thus, it is necessary to accurately estimate the energy consumption behaviour of the WSN system when the new techniques and algorithms are proposed. The low of energy consumption of C_QSE with existing QSE is shown in fig 4.

### E. Average Delay

In wireless sensor network, applications require a congestion control mechanism to regulate the large amount of traffic to inject within WSN to avoid packet loss and to assurance end to end reliable packet delivery. The basic aim of the random access network is to protect ac cess to channel in order to achieve the entire network performance. The arrival rate is a parameter which effects on the traffic at each node that should be controlled properly in order to avoid increasing queue sizes and packet delays. The speed control may be performed either at each node or only at the source of the traffic. Such parameters can effect on whole network performance including the delay, energy consumption, and transmission rates of the packets. The lowaverage delayrate of C_QSE in comparison with QSC is shown in fig 5.

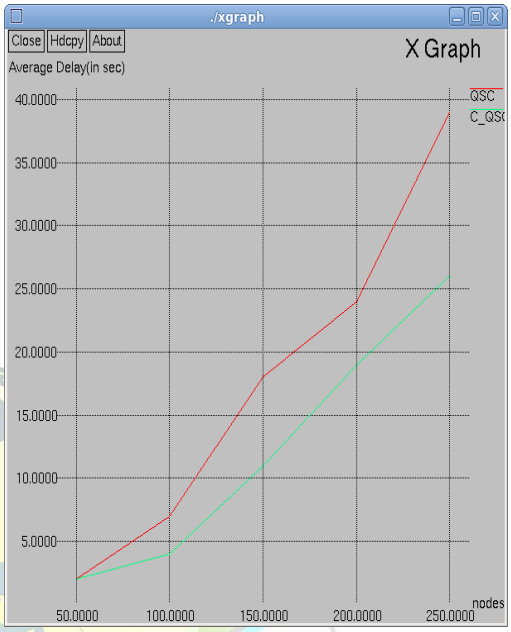



Fig 5: Average delay versus number of nodes in C_QSC & QSC

## IV. Conclusion

A measurement campaign for q-s composite with channel-based key generation was performed.Successful key generation was always possible for the legitimate nodes, with slightly higherkey generating rates. Interception of the keys by theeavesdropper is impossible as illustrated in the evaluation section. In case the eavesdropper knows allthe details of the system and intercepts all data, only limited information about the key couldbe retrieved in the worst-case scenario, potentially slightly decreasing the time needed for a successfulbrute force attack. The analysis results also show that, the proposed scheme can achieve better node life time, have less control overhead, average throughput and average delay in comparison with the exciting q-s composite scheme.

## References

[1] Haowen Chan Adrian Perrig Dawn Song “Random Key Predistribution Schemes for Sensor Network,” in Proc.Carnegie Mellon University.

[2] A. A. Rezaee, M. H. Yaghmaee, A. M. Rahmani, and A. H.Mohajerzadeh, “Hoca: Healthcare aware optimized congestion avoidance and control protocol for wireless sensor networks,” *Journal of Network and Computer Applications*, vol. 37, pp. 216 – 228, 2014. 1992.

[3] X. Du and H.-H. Chen, “Security in wireless sensor networks,” *Wireless Communications, IEEE*, vol. 15, no. 4, pp. 60–66, Aug 2008.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

[4] M. A. Simpl´ıcio-Jr., P. S. Barreto, C. B. Margi, and T. C. Carvalho, "A survey on key management mechanisms for distributed wireless sensor networks," *Computer Networks*, vol. 54, no. 15, pp. 2591– 2612, 2010.

[5] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Symposium on Security and Pri-vacy.*, May 2003, pp. 197–213.

[6] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in *Computer and communications security: CCS '02, 9th ACM conf. on*, 2002, pp. 41–47.

[7] Filippo Gandino, Renato Ferrero and Maurizio Rebaudengo, Senior Member, IEEE, "A Key Distribution Scheme for Mobile Wireless Sensor Networks: q-s-composite," IEEE transactions on information forensics and security,1556-6013(c) 2016 IEEE

[8] Chen, C.; Jensen, M. Secret key establishment using temporally and spatially correlated wireless channel coefficients. IEEE Trans. Mob. Comput. **2011**, 10, 205–215.

[9] Premnath, S.N.; Jana, S.; Croft, J.; Gowda, P.L.; Clark, M.; Kasera, S.K.; Patwari, N.; Krishnamurthy, S.V.Secret key extraction from wireless signal strength in real environments. IEEE Trans. Mob. Comput. **2013,**12, 917–930

[10] Mahmood, A.; Jensen, M.A. Impact of propagation on the vulnerability of channel-based key establishment. IEEE Trans. Antennas Propag. **2016**, 64, 1578–1583.

[11] Van Torre, P.; Castel, T.; Rogier, H. Encrypted body-to-body wireless sensor node employing channel-state-based key generation. In Proceedings of the 10th European Conference on Antennas and Propagation (EuCAP), Davos, Switzerland, 10–15 April 2016; pp. 1–5.