Secure Hybrid DFCMT scheme for Dynamic Routing in Wireless Sensor Networks

Ram Pradheep Manohar and E Baburaj

Research Scholar, Research Scholar, St.Peter's University, Chennai
Professor, Sun College of Engineering and Technology, Nagercoil

Summary
With the appearance of Wireless Sensor Networks (WSN) and its applications created as of late, security has been a noteworthy sympathy toward these force requirement frameworks. As wireless sensor systems (WSNs) keep on developing, so does the requirement for viable security components. Planning cost-productive, secure system conventions for Sensor Networks is a testing issue in light of the fact that sensors are asset restricted wireless gadgets. In this paper, a vitality effective correspondence structure for WSN that significantly streamlines the quantity of transmissions required for keying and rekeying. The principle security prerequisite for WSN applications systems is giving aggregate security along the in preparing procedures of element steering. Keeping in mind the end goal to give the security level, we proposed to incorporate the Probabilistic homomorphic encryption plans alongside element steering. Further, this instrument keeps vindictive nodes from infusing false packets into the system. Consequently, an one-time dynamic key is utilized for one packet just and distinctive keys are utilized for the progressive bundles of the stream. The moderate nodes along the way to the sink can confirm the validness and uprightness of the approaching bundles utilizing an anticipated estimation of the key created by the sender's chance vale, in this manner requiring no requirement for particular rekeying messages packet.

Keywords:
Security, WSN Security, resource constrained device, RC4, Encryption

1. Introduction

Quickly created WSN innovation is no more incipient and will be utilized as a part of an assortment of utilization situations. Commonplace application territories incorporate natural, military, and business undertakings. In military, for instance, the quick arrangement, self-association, and adaptation to internal failure Characteristics of sensor systems make them an extremely encouraging detecting procedure for military charge, control, correspondences, processing, knowledge, observation, surveillance, and focusing on frameworks. In wellbeing, sensor nodes can likewise be conveyed to screen patients and help debilitated patients. Some other business applications incorporate overseeing stock, observing item quality, and checking hazardous situations [1][11]. Future enhancements in innovation will bring more sensor applications into our day by day lives and the utilization of sensors will likewise advance from only catching information to a framework that can be utilized for constant compound occasion cautioning. From a security point of view, it is essential to give valid and exact information to encompassing sensor nodes and to the sink to trigger time-basic reactions (e.g., troop development, clearing, and first r In any case, securing sensor systems postures one of a kind difficulties to convention manufacturers on the grounds that these small wireless gadgets are conveyed in huge numbers, as a rule in unattended situations, and are seriously restricted in their abilities and assets (e.g., power, computational limit, and memory). Thusly, convention developers must be mindful about using the constrained assets installed the sensors proficiently. In this paper, we concentrate on keying instruments for WSNs. There are two central key administration plans for WSNs: static and element. In static key administration plans, key administration capacities (i.e., key era and circulation) are taken care of statically. That is, the sensors have a settled number of keys stacked either before or soon after system organization [16].

Then again, dynamic key administration plans perform keying capacities (rekeying) either occasionally or on interest as required by the system. The sensors powerfully trade keys to convey. Albeit dynamic plans are more assault strong than static ones, one huge impediment is that they build the correspondence overhead because of keys being invigorated or redistributed every once in a while in the system [8]. There are numerous explanations behind key refreshment, including: redesigning keys after a key renouncement has happened, reviving the key such that it doesn't get to be stale, or changing keys because of element changes in the topology[15]. In this paper, we try to minimize the overhead connected with reviving keys to keep away from them getting to be stale. Since the correspondence expense is the most overwhelming element in a sensor's vitality utilization, the message transmission cost for rekeying is a vital issue in a WSN arrangement (as broke down in the following area). Besides, for certain WSN applications (e.g., military applications), it might be essential to minimize the quantity of messages to diminish the likelihood of identification if conveyed in an adversary region. That is, by and large less "loquacious" instinctively diminishes the quantity of chances for noxious substances

Manuscript received January 5, 2016
Manuscript revised January 20, 2016

to listen in or capture bundles. This paper gives a strategy to check information in line and drop false bundles from pernicious nodes, in this way keeping up the soundness of the sensor system. In addition it progressively redesigns keys without trading messages for key reestablishments and inserts uprightness into packets rather than appending so as to augment the bundle message validation codes (MACs) [13]. In particular, each detected information is ensured utilizing a basic RC4 encryption plot and sent toward the sink. The way to the encryption conspires progressively changes as an element of the time estimation of the sensor, therefore requiring no requirement for rekeying. Hence, an one-time dynamic key is utilized for one message produced by the source sensor and diverse keys are utilized for the progressive bundles of the stream. The nodes sending the information along the way to the sink can confirm the genuineness and honesty of the information and to give no denial [14]. The convention can proceed with its operations under critical correspondence cases as it might be working in a high-blunder inclined organization zone like submerged.

2. Background and motivation

One huge part of secrecy examination in WSNs involves outlining productive key administration plans. This is on account of dent of paying little mind to the encryption system decided for WSNs, the keys must be made accessible to the imparting nodes (e.g., sources and sink(s)). The keys could be disseminated to the sensors before the system arrangement or they could be redistributed (rekeying) to nodes on interest as activated by keying occasions. The previous is static key administration [2] and the last is rapid key [3][12] administration. Rekeying with control messages is the methodology of existing element keying plans though rekeying without additional control messages is the essential element of this paper existing element key-based plans spend a lot of their vitality transmitting rekeying messages. With this perception, this paper is propelled to give the same advantages of element key-based plans, yet with low vitality utilization [9]. It doesn't trade additional control messages for key reestablishment. The keys are powerful taking into account time estimation of sensor and in this way one key for each bundle is utilized. This makes stronger to specific assaults (e.g., replay assaults, savage power assaults, and disguise assaults).

3. Proposed framework overview

The proposed framework is organized into four phases. They are Time Based Keying, encryption, Filtering and Forwarding, Dynamic Routing.

3.1 Time Based Keying

One of the essential commitments of the proposed system is the era of keys powerfully utilizing neighborhood time. It creates a dynamic key that is then encouraged into the encryption module. At the point when a source node has information to send to the sink because of either an outer incitement by the sink or a self-started occasional report, it utilizes its neighborhood clock esteem as the key. In particular, the keys are a component of the present time esteem (tl) and an introduction vector (IV).
Function used for Timed Based Key Generation:

Kt j _ F (tl, IV) (1)

Algorithm 1: Compute Dynamic Key

```
1:ComputeDynamicTimeKey(t1)
2:begin
3:j ß txcnt
4:if j=1 then
5:Kj=F(t1 ,IV)
6:return Kj
7:end
```

Dynamic Time based entering is given in calculation 1. For instance, expect the source node is N1, and the forwarder nodes N2 and N3 are on the way to the sink that the report by N2 will navigate. Note that N1 embeds a duplicate of its ID and a nearby counter esteem inside the report (bundle) sent to the sink. The counter serves as an assurance against replay assaults. It is expanded every time a packet is sent from the source. The ID is utilized to check the respectability of the packet. N1 utilizes its nearby clock esteem 16 as the key. This key is utilized by the Encryption stage to perform the wanted secretive operations relying upon the security administration (e.g., encryption, validation, trustworthiness) gave by the WSN application. At the point when N2 gets the report from N1, it tries to discover the estimation of the time at N1. To start with N2 subtracts the rough bundle flight time (È= ñ + ô + å + ö) in the middle of itself and N1 from its nearby time so as to be closer to the neighborhood time at N1, where ñ is the engendering time, ô is the packet transmission time, ö is the bundle preparing time, and å is the estimation of mistakes for variability in transmissions because of blurring, hindrances, and programming blunders, and so forth. Moreover, all together for a forwarder node to locate the nearby time esteem at the source node effortlessly, all nodes are connected with a window of qualities, which we allude to as the tick window; (Tw) and tick esteem (Ö). Subsequently, N2 will attempt all qualities inside its tick window starting from its neighborhood clock esteem. Once N2 finds the right key worth connected with the time at N1, utilizing the discovered key, it will have the capacity to perform other security activities on the packet in the encryption module and will likewise have the capacity to

register the time counterbalance from the sender. Nonetheless, to battle against fake qualities and to guarantee a forwarder node does not endeavor to beast compel untouched based keys, lower and upper limits are connected with every node's ti

3.2 Encryption

Because of the asset imperatives of WSNs, conventional advanced marks or encryption systems requiring costly cryptography is not suitable. The plan must be basic, yet successful. So in this stage a straightforward encoding operation is utilized. The encoding operation is basically the procedure of stage of the bits in the bundle, as per the progressively made change code by means of the RC4 encryption system. The way to RC4 is made by the past module (time-based keying). The reason for the encryption module is to give basic privacy of the bundle header and payload while guaranteeing the legitimacy and uprightness of detected information without acquiring transmission overhead of conventional plans. The bundles comprises of the ID (i-bits), sort (t-bits) (expecting every node has a sort identifier), and information (d-bits) fields. Every node sends these to its next jump. Then again, the sensors' ID, sort, and the detected information are transmitted in a pseudorandom style as indicated by the consequence of RC4. All the more particularly, the RC4 encryption calculation takes the key and the bundle fields (byte-by-byte) as inputs and creates the outcome as a stage code as portrayed in Fig.1. The link of each8-bit yield turns into the resultant stage code [4]. The resultant stage code is utilized to encode the {ID, sort, data} message. At that point, an extra duplicate of the ID is likewise transmitted free alongside the encoded message. The configuration of the last packet to be transmitted gets to be Packet= {ID, {ID, sort, data} Pc} where {x}k constitutes encoding x with key k. Two operational modes utilized as a part of the Encryption stage to decide how to forward the approaching packet can be imagined. In the first mode, No-re Encode mode, the first approaching packet is sent to the upstream node with no re-encryption though in the second mode, re Encode mode, the approaching bundle is sent to the upstream node after re-encryption with the key connected with the nearby time at this collector node. For re Encode mode, the forwarder node utilizes its present nearby clock esteem and IV quality to make another key when re-encryption the approaching packet. The upside of the No-re Encode mode is one encryption calculation; subsequently vitality is spared by sending the first bundle. This is the prescribed method of operation. On the other hand, if the present sending node is found too far from the source node, the sending node might order a solid approaching bundle as pernicious. In particular, this case happens if the time distinction between the nearby times of the source and the faraway node is greater than the aggregate time secured with Tw _ Ö. In any case, this is not an issue for re Encode mode in light of the fact that the forwarder nodes revive the key, used to encode the sent packet. Inevitably, in both modes when the sink gets the report along the way, it likewise experiences the same keen key-discovering technique as forwarder nodes

3.3 Hybrid ph scheme

The researchers did experiments on the suitable homomorphic algorithms in terms of the possible attacks and low security level. The successful combination of Domingo-Ferrer(DF) and Castelluccia Mykletun Tsudik (CMT) schemes which increases the security and the minimization of overhead. The next approach manages specific disadvantages by considering homomorphic message authentication codes. In order to do the cascade encryption, the researchers integrate the CNT with the concealed Data aggregation (CDA). The inner encryption is CMT whereas the outer encryption is DF and the knowledge of the secret key is needed to modify the content of the single data packet. The computational complexity requirement is same as the standalone DF is the advantage of this scheme.

3.4 .Dynamic Routing

The Hybrid PH scheme is implemented along with AODV routing protocol [5][6] to offer routing security. Such schemes are seeing deployment as part of one-hop 802.11 networks; RC4 and HPH schemes are deployed and certificates are carried by nodes. New AODV scheme consists of a preliminary routing process followed by a route instantiation process that guarantees end-to end authentication. The protocol is simple compared to most non-secured sensor routing protocols. It should be noted that the exploits the optimizations that have been introduced into ad hoc routing protocols for route computation and creation. Route discovery in New AODV process is accomplished by a broadcast route discovery message from a source node which is replied to unicast by the destination node, such that the routing messages are authenticated at each hop from source to destination, as well as on the reverse path from the destination to the source.

Algorithm

1. The step involves registration of all SNs within the individual clusters in order to generate their respective ID tables at the headnodes.
2. Generate the ID slot, in which it addresses the ID issues of the original CMT schemes.
3. The ID transformation is then forwarded to the RMS via the gateway node over the Backbone network

4. Each cluster and their respective keys used by the individual SN along with the aggregate function is the forwarded, in the form of cipher text.
5. Once, all the above steps are completed CH node broad casts a CTS signal to all its SNs. Each sensor node encrypts their encryption key Ki and forward encrypted sensor data to its CH node.

3.5 Filtering and Forwarding

The sifting and sending eliminate channels the noxious information of the system if the approaching bundle is malignant or advances the information toward the sink generally. Note that the first bundle is not amplified at all (e.g., with MACs) to keep the vitality costs at least however much as could be expected.

Forwarder Node Algorithm

Once the sending node gets the packet and validates the message by interpreting the message and contrasting the plaintext node ID and the encoded node ID. On the off chance that the bundle is credible, then the node utilizes its nearby time to encode packet and forward it to next jump. On the off chance that the packet is not legitimate it is disposed of.

Dynamic Routing

This module handles dynamic routing and endures disappointments of subjective individual nodes in the system (node disappointment). Way Repair Algorithm [10] is utilized for element routing since it the system can endure node disappointments and highways a message circling the fizzled nodes. The system comprises of four sections:

Failure detection
·Failure information propagation
·New parent detection
·New parent selection.

Initial, a node identifies if its guardian node is alive and if the guardian node can associate with base station. This part is called disappointment discovery. In the event that a node s identifies that its guardian node functions admirably, it won't do any upkeep work [7].On the off chance that there are a few issues in guardian node, for example, node disappointment or separated to base station (potentially one of guardian node's predecessor node is fizzled), node s illuminates its youngsters nodes about the disappointment, which is called disappointment data spread. Moreover, s asks for the association data from its neighbor nodes since it needs to pick another guardian node from them. This part is called new parent recognition. In the wake of gathering data from its neighbor nodes, s chooses another guardian node taking into account the data it gathered. This part is called new parent choice. We indicate an as the node who tries to keep up its course way. Node p (a) will be a's guardian node.

1. Node a sends FORWARD message to its guardian node p(a) , and set a timeout (timeout_ppt) for BACK message fromp(a). FORWARD: a à p (a)
2. On the off chance that p (a) gets the FORWARD message, it will answer a BACK message. The BACK
Message contains the data that whether p
(an) associate with base station or not, and in the event that it is joined, the bounces to base station. In the event that p (a) unites with base station, it sends BACK_YES message back to a. BACK_ YES: p (a) à a: connect||hops If p (a) can't unite with base station, it sends BACK_NO message back toa:
(a) can't join with its guardian node p.parent, the p.broken_hops is set to 1. Something else, p.broken_hops= p.parent.broken_hops + 1
3(a). On the off chance that a gets BACK_YES from p (an), aresets its bounces as guardian p's jumps in addition to one:ahops à jumps + 1. In the event that a node's bounces past a greatest limit esteem, it sets itself detached: ahops ß _.
(b). In the event that p (an) is dead or its sign is blocked, it can't answer BACK message inside timeout. In the event that a can't get BACK message from p (a)within the predefined timeout, a realizes that it can't interface with base station through p (a). At that point it shows a R_REQUEST message to the greater part of its neighbor nodes to locate another guardian node. R_REQUEST: aà NEIGHBOR: ask for guardian

(c). In the event that a gets BACK_NO from p (an), realizes that p (a) can't interface with base station right then and there. Rather than TV R_REQUEST message instantly, a holds up a timeout before sending R_REQUEST. The timeout relies on upon the estimation of broken_hops from BACK_NO message. This technique gives guardian node p some an opportunity to locate its new parent node. a will set its broken_hop, and proliferate it when its youngsters nodes send FORWARD message to a.
4. At the point when one of a's neighbor node n gets R_REQUEST message from an, and if n can associate with base station, it sends a R_REPLY message back to a. R_REPLY message contains the ID of n's guardian node, and n's bounces to base station: R_REPLY: n à a: connect||n_hops||n.parent If n can't interface with base station, it won't send any message back to a. Rather, it records an as one of its R_REQUEST senders. On the off chance that has not got any R_REPLY message from its neighbor nodes, it will resend R_REQUEST after a specific timeout.
5. At the point when a gets R_REPLY messages from its neighbor nodes, if the R_REPLY message says that the sender unites with base station, arecords the sender as a guardian competitor. At last, a chooses its new parent node whose jumps to base station is littlest among all applicants.

After it chooses guardian node, sets its jumps as its parent node's bounces in addition to one: Ahopsß p (a) boun

3.6 Time Uncertainty

Uncontrolled ecological conditions, for example, changes of temperature, dampness, weight, and sudden vibrations in the sending region on the grounds that interior tickers to step by step wander from the genuine clock. Also, channel access time (at the medium access control layer) and send-time (counting the ideal opportunity for setting up the bundle at the application layer and passing it to the lower layers), can be considered as adding to the erratic timekeepers.
Instability Parameters In this paper, the ecological elements are caught with the parameter ä, which is the day by day estimation of the float per sensor given an arrangement region; while the product based components are caught with å. Deterministic variables, then again, rely on upon more unsurprising parameters. These incorporate the transmission time of one bundle (ô), the engendering delay (ñ), the packet preparing time (ö) (e.g., because of cryptographic operations), and the normal time of information from sensors (ë). The vulnerability parameters I adapting to deterministic and non-deterministic elements are condensed in fig.2. The impact of the considerable number of components is caught by the tick window, Tw, and it is the most noteworthy parameter in managing the instability. It gives a window of time equal

3.7 The Choice of Tw

The tick window Tw is accessible for the beneficiary node to browse to decipher the got packets. The window has upper and lower limit values. The viability of the proposed convention relies on upon the extent of this window in light of the fact that the bigger the span of Tw, the additional time it takes for a collector to locate the key. The Tw worth is essentially a component of the tick esteem (Ö). The littler the estimation of the tick, the more keys could be attempted by every sensor, thus Tw is bigger and the precision of the plan is expanded. Likewise, from the sender's point of view, as the framework turns out to be more exact (i.e., the littler the tick esteem), the shot of utilizing an alternate key for every bundle transmitted expansions. For whatever length of time that the recurrence of the occasions (bundles) is bigger than 1/Ö, the framework will utilize an alternate key for each packet

4. Performance analysis

In this segment, the vitality exhibitions of proposed "Time Based Keying" and other existing plans (SEF [6], DEF [8]) are dissected. To start with, we quickly condense every convention and talk about their disadvantages. At that point, the examination results are displayed. Ye et al., proposed factual in transit sifting (SEF) [6].In SEF, every detecting report is accepted by different keyed message confirmation codes. In particular, every node is furnished with some number of keys that are drawn haphazardly from the worldwide key pool. Initial, a focal point of boost is chosen among the source sensor nodes in the occasion locale. At that point, once a report is produced by a source node, a MAC is annexed to the report. Next, another upstream node that has the same key as the source can check the legitimacy of the MAC and channels the bundle if the MAC is invalid. Then again, the drawback of SEF is that the nodes must store keys and bundles are broadened by MACs. Despite the fact that the creators propose the utilization of blossom channels to diminish the MAC overhead, SEF is a static key-based plan and it acquires every one of the drawbacks of static key administration plans. In the Dynamic En-course Filtering (DEF) plan by Yu and Guan [8], a real report is supported by numerous detecting nodes utilizing their own validation keys. Before arrangement, every node is preloaded with a seed validation key and l +1 mystery keys haphazardly looked over a worldwide key pool. Before sending reports, the bunch head disperses the verification keys to sending nodes scrambled with mystery keys that will utilize for embracing. The sending nodes store the keys on the off chance that they can decode them effectively. Later, group heads send confirmation keys to approve the reports. The DEF plan includes the use of validation keys and mystery keys to spread the verification keys; thus, it utilizes numerous keys and is confounded for asset constrained sensors.

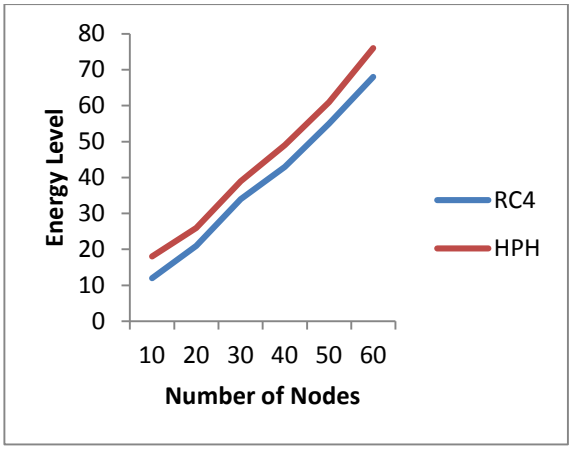

Figure 1 Energy level variation

An examination of existing plans and HPH scheme as far as their vitality utilization is exhibited in Fig. 1. The outcomes are produced for one round of correspondence from a source node to the sink, which is thought to be found n bounces far from the source node. The x-pivot speaks to the bounce number and is changed, while the y-node is the

vitality. The outcomes show vitality productivity of the proposed time based keying plan.

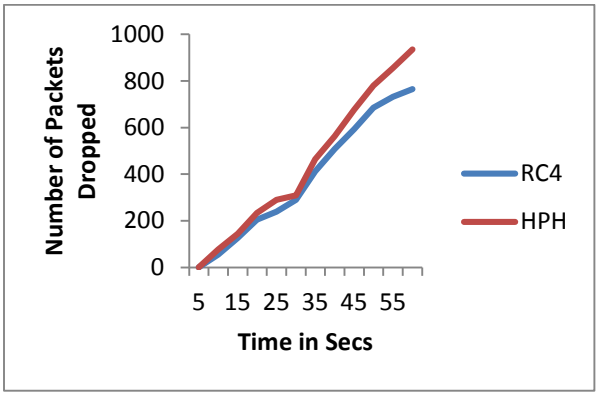

Figure 2 Ratio of Packets Dropped

5. Conclusion

Correspondence is expensive for wireless sensor systems (WSNs) and for certain WSN applications. Free of the objective of sparing vitality, it might be vital to minimize the trading of messages (e.g., military situations). Timed based keying produces one of a kind key every time so progressive bundles of the stream use distinctive keys making stronger to specific assaults (e.g. replay assaults, animal power assaults, and disguise assaults). Key era is started when information is detected and in this manner no unequivocal component is expected to invigorate or upgrade keys so we can spare vitality. In addition, the dynamic way of the keys makes it troublesome for assailants to capture enough packets to break the encoding calculation. A Dynamic finding routing technique for correspondence between sensor nodes and a base station in a WSN is additionally displayed. This technique endures disappointment of discretionary individual nodes in the system or a little part of the system by progressively finding new courses when nodes fall flat. The proposed component is nonspecific as in it can be incorporated in a few routing conventions to make them flaw tolerant. The execution investigation of the proposed structure with other existing plans indicates better results if there should be an occurrence of adaptation to non-critical failure and spares vitality. Future work will address maintaining a strategic distance from correspondence overhead while performing dynamic routing and insider assaults.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E.Cayirci, “Wireless Sensor Networks: A Survey,” Computer Networks, vol. 38, no. 4, pp.393-422, Mar.2002.

[2] L. Eschenauer and V.D. Gligor, “A Key- Management Scheme for Distributed Sensor Networks,” Proc. Ninth ACM Conf. Computer and Comm. Security, pp. 41-4,2002.

[3]]M. Eltoweissy, M. Moharrum, and R. Mukkamala,“Dynamic Key Management in Sensor Networks,” IEEE Comm. Magazine, vol. 44, no. 4, pp. 122-130, Apr. 2006.

[4] Crossbow Technology, http://www.xbow.com, 2008.[6] F. Ye, H. Luo, S. Lu, and L. Zhang, “StatisticalEn-Route Filtering of Injected False Data in Sensor Networks,” IEEE J. Selected Areas in Comm., vol. 23, no. 4, pp. 839-850, Apr. 2005.

[5] Jaydip Sen, Arijit Ukil “ A Secure Routing Protocol for Wireless Sensor Networks”, Computational Science and Its Applications – ICCSA 2010 Volume 6018 of the series Lecture Notes in Computer Science pp 277-290.

[6] Soumyashree Sahoo , Pradipta Kumar Mishra and .Rabi Narayan Satpathy3Secure Routing in Wireless Sensor Networks IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012.

[7] S. Uluagac, C. Lee, R. Beyah, and J. Copeland,“Designing secure protocols for sensor networks,” Lecture Notes in Computer Science, Algorithms, Systems, and Applications (WASA)., vol. 5258, pp. 503–514, 2008.

[8] Z. Yu and Y. Guan, “A DynamicEn-Route Scheme for Filtering False Data Injection in Sensor Networks,” Proc. IEEE INFOCOM, pp. 1-12, Apr. 2006.

[9] A. S. Uluagac, R. A. Beyah, and J. A. Copeland, “TIme-Based dynamic keying and en- route filtering (TICK) for sensor networks,” Submitted to IEEE Globecom 2010 - Communication & Information System Security, Miami, Florida, USA.

[10] Prof. Arabinda Nanda, Prof (Dr) Amiya Kumar Rath, Prof. Saroj Kumar Rout, “Node Sensing & Dynamic Discovering Routes for Wireless Sensor Networks” (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 3, March 2010.

[11] M. Li, W. Lou, and K. Ren, “Secure device pairing,” in Encyclopedia of Cryptography and Security (2nd Ed.), H. Tilborg and S. Jajodia Ed., Springer, to appear, 2010

[12] K. Naga Krishnaja, “Cryptography via Virtual Energy for Wireless Sensor Networks,” International Journal of Information and Education Technology, Vol. 2, No. 1, February 2012.

[13] Abu Shohel Ahmed, “An Evaluation of Security Protocols on Wireless Sensor Network,” TKK T- 110.5190 Seminar on Internetworking, April 2009.

[14]]S.P. Santosh Kumar, C.B. Sivaparthipan, D. Prabhakar and Dr. S. Karthik, “Secure Encryption Technique with Keying Based Virtual Energy for Wireless Sensor Networks,” Vol. 1, Issue 5, October 2013.

[15] Renu Bala , Yashpal ” Secure Routing in Wireless Sensor Network”, –International Journal for Innovative Research in Science & Technology Volume 2 Issue 01 June 2015. PP 301-308.

[16] Etimad Fadel ,V.C. Gungor, Laila Nassef, ,M.G. Abbas Malik “A survey on wireless sensor networks for smart grid”, Computer Communications , Science Direct, Volume 71, 1 November 2015, Pages 22–33.