VOL. 11, NO. 7, APRIL 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SECURE ENERGY TRADEOFFS WITH LOW POWER CONSUMPTION IN DATA TRANSMISSION OF WIRELESS SENSOR NETWORKS

S. Venkataramana[1], P. V. G. D. Prasad Reddy[1], S. Krishna Rao[2]
[1]Department of CS and SE, Andhra University-Visakhapatnam, Andhra Pradesh, India
[2]Sir CRR Engineering College, Eluru, Andhra Pradesh, India
E-Mail: vrsarella@gmail.com

ABSTRACT

Sensitivity of the Wireless Sensor Networks (WSN) is the main emerging concept in real time application for data transmission and other operations in process of networks. Security in WSN is challenging issue in recent network applications in design and implementation. A new extremely scalable key organization plan for Wireless Sensor Network. For that objective, we create use, for the very first time, of the unital style concept. We assume to extend protocol hierarchy best trade off results in data communication with parameter selection in wireless sensor networks. With a rapid progress of numerous applications in Wireless Sensor Networks (WSNs), performance evaluation and analysis techniques face new challenges in energy efficiency area in WSN applications. One of the key issues is to perform the security trade-off and energy efficiency analysis. In this paper, the energy analysis module for the QoP-ML (quality of protection modelling language) is proposed by means of which one can analyze the influence of various security levels on the energy consumption of a protocol.

Keywords: wireless sensor networks, security, key management, network scalability, source marketing.

1. INTRODUCTION

More particularly, we analyze the maximum quantity of redundancy through which information is directed to a distant sink in the existence of untrustworthy and harmful nodes, so that the question achievements possibility is optimized while maximizing the Heterogeneous Wireless Sensor Networks (HWSN) life-time. But some obstacles interrupted the systems performance differently such as the improving bundle wait, thus difficult for reordering the packages, marketing is not effectively handled and streaming issue in low data transfer usage information, thus reducing performance. To be able to get over the disadvantages of the formerly suggested program, we apply the new idea in this document. In this our suggested program, the best possible contact range and interaction technique were mixture to implement the Heterogeneous Wireless Indicator Networks lifestyle in nature. In HWSN, the intra-cluster arranging and inter-cluster multi-hop redirecting offer to take advantage the network lifetime. And it is regarded as a hierarchal HWSN with CH nodes such as excellent energy and providing out capabilities than regular SNs. Our suggested strategy gives solution to come up with as an optimization problem to balance energy intake across all nodes in the entire heterogeneous sensor systems. Though in this document, we suggest two-tier HWSN with the objective of take advantage on network life-time while satisfying energy control and coverage goals.

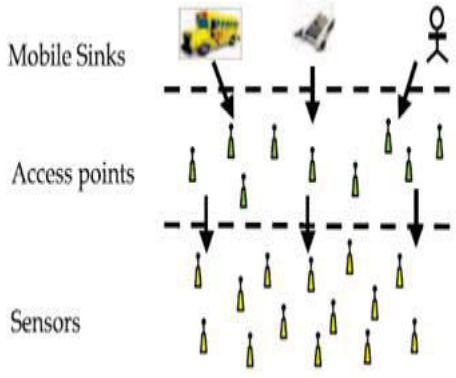

Figure-1. Wireless mobile node communications with secure data.

Key management is an area stone service for many security alternatives such as comfort and verification which are required to secure emails in WSN [3][7]. The company of secured links between nodes is then a complex problem in WSN. The group key based alternatives, which provide effective key management services in conventional techniques, are unsuitable for WSN because of resource limitations. Some group key techniques have been used on real receptors. Shaped key company is then one of the most appropriate paradigms for acquiring dealings in WSN [8].

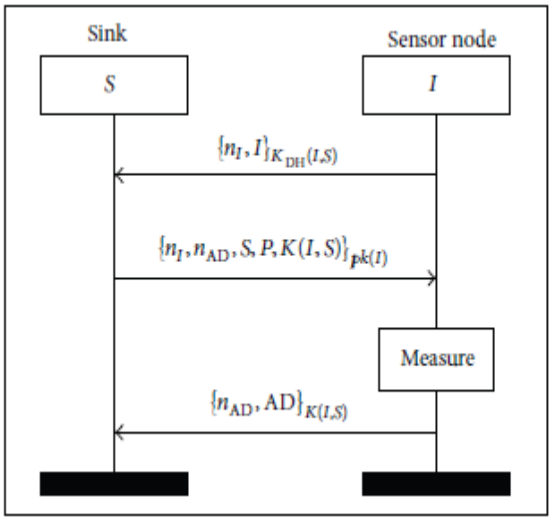

Figure-2. Energy saving hierarchy in wireless sensor networks.

Current analysis performs either allow to back up a low wide range a nodes or crack down the other system actions such as resiliency, relationship and storage area space cost when the wide range of nodes is important. As opposed to these alternatives, our purpose is to enhance the scalability of WSN key management methods without degrading significantly the other system actions. To achieve this purpose, we suggest using, for initially, the unital design to make and pre-distribute key jewelers. First, we explain the unital design and we suggest a primary implementing from unital to key pre-distribution for WSN. Designing protected methods which fulfil the required efficiency is an essential issue to be fixed. The traditional strategy represents that the best way is to apply the most powerful possible protection systems, which make the program as protected as possible. Energy-efficient alternatives are always calculated and in contrast to types [9]. Dimensions can be done either by tests or models. As the first solution is in many situations quite hard to execute the simulator is used instead [12]. There exist many assessment techniques, such as data or pieces circulation research, the condition conversion modelling depending on Markov sequence, and Petri net or model-driven structure research [14]. However, the traditional writers point out that most of traditional power designs are generally oversimplified and concentrate only on RF transceivers neglecting other components, what may result in obscure assessment especially when considering the situations with heavy workloads on processer chips and receptors. They recommend an event-driven lining up Queueing Petri Net (QPN) style to imitate the power intake actions of indicator [13,14]. The QPN style allows us to assess the power intake of indicator, transceiver, and processer models such as their condition changes [15].

The main efforts of this document are described as follows.

(i) We recommend an expansion of the QoP-ML which allows us to accomplish a complicated program research as part of method efficiency research. Furthermore, we present a high level interaction component, which during the research considers the following elements: program topology, redirecting, and packet filtration. This new component eliminates all the above-listed restrictions of the QoP-ML.

(ii) We recommend an energy-efficiency component by means of which one can assess the impact of given operations on power intake and program life-time.

(iii) The two segments presented in this document are implemented in the Automated Quality of Protection Analysis Tool (AQoPA). The AQoPA works automatic evaluation and marketing of complicated program models created in QoP-ML.

(iv) We existing a research of energy-efficiency analysis and protection trade-offs for a complicated wireless sensor network. Using this example, we want to present a method to find a trade-off between protection and energy efficiency. The research is depending on an existing WSN implemented on the Jindo Link in South Korea.

The remainder of this paper organizes as follows: Section II describes related work of secure key distribution in data transmission in wireless sensor networks. Section III explains briefly the components of the QoP-ML terminology. In Section IV, a new interaction design and its functions and structures are described. In Section V, the power research component is explained, and in Section VI, we existing a research which uses the new performance of the presented communication model.

2. RELATED WORK

Elliptic curve cryptography in WSNs: The principle thought is that for every message m to be discharged, the message sender, or the sending hub, produces a source unknown message authenticator for the message m. The era depends on the Modified ElGamal Signature (MES) plan on elliptic bends. For a ring signature, every ring part is required to register a fabrication signature for every other part in the Ambiguity Set (AS). In our plan, the whole Source Anonymous Message Authentication (SAMA) era requires just three stages, which connect all non-senders and the message sender to the SAMA alike [1]. What's more, our outline empowers the SAMA to be confirmed through a solitary mathematical statement without exclusively checking the marks.

Let p > 3 is an odd prime. An elliptic bend E is characterized by a mathematical statement of the structure:

$$E: b^2 = a^3 + xa + x \bmod p,$$

$where a, b \in F_p, and 4a^3 + 27b^2 \# 0 \bmod p$ [4]. The set E (F) consist of all points (a, b)∈ on the curve, together with a special point O, called the point at infinity. Let G =(xG; yG) be a base point on E(Fp) whose order is a very large value N. User A selects a random integer dA [1,N-1] as his private key. Then, he can compute his public key QA from QA = dA X (G).

Signature generation procedure: If user sends some information to destination then that message is encrypted with semantics in wireless sensor networks. Then the following procedure will be performing on recommended conditions:

Select a random integer k_A $1 \le k_A \le N-1$.

Calculate r = $x_A \bmod N$ where $(x_A, y_A) = k_A G$

If r = 0, go back to step 1.

Calculate hA<---h(m; r), where h is a cryptographic hash function, such as SHA-1, and <---- denotes the l leftmost bits of the hash for providing security.

3. KEY MANAGEMENT AND COMPROMISED NODE DETECTION

In our plan, we accept that there is a Security Server (SS) whose obligations incorporate open key stockpiling and conveyance in the WSNs. We accept that the SS will never be bargained. Be that as it may, after organization, the sensor hub may be caught what's more, traded off by the aggressors. Once compromised, all data put away in the sensor hub will be available to the aggressors. We further expect that the traded off hub won't have the capacity to make new open keys that can be acknowledged by the SS. For proficiency, every open key will have a short personality. The length of the personality depends on the size of the WSNs.

Compromised Node Detection [1] as an uncommon situation, we expect that all sensor data will be conveyed to a sink hub, which can be collocated with the SS. As discussed in above, when a message is gotten by the sink hub, the message source is covered up in an AS. Since the SAMA plan ensures that the message uprightness is un-tampered, when a terrible or pointless message is gotten by the sink hub, the source hub is seen as traded off. In the event that the traded off source hub just transmits one message, it would be extremely troublesome for the hub to be recognized without extra system movement data. Nonetheless, when a bargained hub transmits more than one message, the sink hub can contract the conceivable traded off hubs down to a little set. In our plan, we accept that there is a SS whose obligations incorporate open key stockpiling and conveyance in the WSNs. We accept that the SS will never be bargained. Be that as it may, after organization, the sensor hub may be caught what's more, traded off by the aggressors. Once compromised, all data put away in the sensor hub will be available to the aggressors.

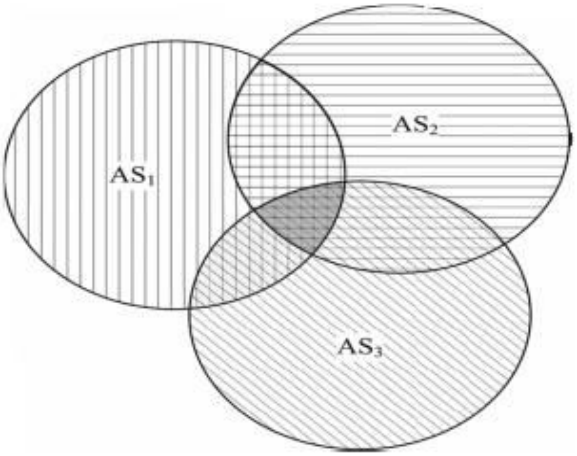

Figure-3. Compromised node detection.

We utilize the circle to speak to an AS. At the point when one and only message is transmitted, the sink hub can just acquire the data that the source hub will be in a set, say AS1. At the point when the traded off source hub transmits two messages, the sink hub will have the capacity to limit the source hub down to the set with both vertical lines and even lines. At the point when the traded off source hub transmits three messages, the source hub will be further limited down to the shaded range. Subsequently, if the sink hub continues following the traded off message; there is a high likelihood that the bargained hub can be disconnected.

4. PROPOSED APPROACH

In the paper [2], Ksiezopolski presents the top high quality of security acting terminology, which provides the acting terminology to make abstraction of cryptographic methods with concentrate on the important points concerning the top high quality of security. The developed use of the QoP-ML is to indicate a series of activities described as a cryptographic technique. The QoP-ML has presented a multilevel technique research which increases the chance of describing the condition of a cryptographic technique.

General view: Elements used in the QoP-ML represent an innovative stage of abstraction which allows us to pay attention to the high quality of security research. The QoP-ML includes of processes, functions, idea applications, aspects, and QoP statistics. Techniques are globally factors organized into the main procedure, which symbolizes only one pc (host). A procedure identifies activities, functions represent only one function or a number of functions, and applications figure out the environment in which a procedure is applied.

Data types: In the QoP-ML, an endless set of factors is used for describing interaction applications, procedures, and functions. Factors are used to shop information about the program or a particular procedure. The QoP-ML is a very subjective acting terminology, so there are no unique information kinds, dimensions, or value differs. Factors do not have to be declared before they are used. They are immediately declared when they are used for initially.

Features: Program behaviour is customized by functions which change the states of aspects and successfully pass factors by communication applications. When decoding a function, one has to set the explanations of this function which explain two kinds of aspects. Efficient aspects released in round supports are necessary for the performance of a function while other elements released in rectangular shape supports impact the program high quality of security.

Protection analytics: Program activities, which are officially described by a cryptographic technique [5,6], can be made by the suggested QoP-ML. One of the primary is developed of this terminology is to very subjective the high top high quality of security of a particular version of the analyzed cryptographic technique. In the QoPML, the impact of program security is showed by means of functions. While introducing a function, the high quality of security aspects is determined and the important points about this function are described. These aspects do not impact the flow of a technique, but they are essential for the high quality of security research.

5. ENERGY ANALYSIS IN WSNs USING QoPML

The aim of the power research component is to examine the power intake of the made system. Energy intake is measured as the sum of the power absorbed by simple functions which use only the CPU (security functions, other mathematics functions, etc.) and interaction functions (listening, receiving, and sending) which use the radio. The power intake of one CPU or interaction operation is measured as follows:

$$E_{op} = T * I * V$$

Where E_{op} is the power intake of CPU or communication operation, op is the catalog of function, T is plenty of your energy of the function,

I is the electricity of the function, and V is the volts of the variety.

Lastly, the power component research analyzes the energy consumption for each variety as follows:

$$E_H = E_{H_{CPU}} + E_{H_{COMM}}$$

The energy research component presents three parameters: sending present, getting present, and hearing present. All of them explain the electricity in three different declares. The hearing present describes the electricity when a host holds back on the route for a concept. The electric current in the transmitting state has been separated in two: the sending present and the getting present because serves can send and receive data with different power voltages (e.g., the sending present in the receptors can differ based upon on signal strength).

Algorithm 1: Communication operations with deterministic CPU utilization.

```
(1) communication {
(2) medium[wsn] {
(3) default q = 1;
(4) default t = 20ms;
(5) default sending current = 14.8 mA;
(6) default receiving current = 22.4 mA;
(7) default listening current = 1.8 mA;
(8) topology {
(9) Sensor <->Gateway : sending current =
wsn sending current[mA];
(9) }
(10) }
(11)}
```

The nodal life time NL (G,v) of node V in the system showed by chart G is described as follows:

$$nl(G,v) = \frac{E_r(v)}{E_{cpu}(v) + Ecomm(v)}$$

Where E(V) indicates the recurring power of node V. E CPU(V) and E COMM(V) are the amounts of power of all CPU and the communication functions, respectively, of node V.

The sum of all CPU operations is defined as follows:

$$E_{CPU}(v) = \sum_{i \in CPU} E_i(v)$$

Where CPU is set of indexes of all CPU operations with specified communication property.

The sum of all communication operations is defined as follows:

$$E_{COMM}(v) = \sum_{i \in COMM} E_i(v)$$

Where COMM is communication operations

(Sending, receiving and listening). The trade-off between the protection and power efficiency is obtained by choosing most power effective edition of a method which provides protection at the needed stage in a given device of time.

Acquired results recommend that in some circumstances ensuring security at the trouble of power intake is unavoidable. However, before applying designed alternatives, there is a need to evaluate taken into consideration atmosphere and choose the option which satisfies given specifications best (in terms of, for example, time or power consumption). The suggested strategy cans instantly response the question what is the improvement in efficiency between the created circumstances. Through this research you can make a trade-off between the means of information security and the required efficiency. In addition, this research allows us to make circumstances to deal with a situation that will require greater efficiency or security. Such activities may include a unexpected and important modify of ecological aspects, for example, unexpected climate modify that indicates stronger requirements for efficiency.

6. EXPERIMENTAL EVALUATION

Key control is one of the main problems for secret-key based verification techniques. This is especially real for large range WSNs. Execution time shown in Table-1 follows:

Table-1. Comparison analysis in terms of time.

Clients	QoPML	ECC with SAMA	SAMA
1	1.5	2.4	2.8
2	1.6	2.5	2.9
3	1.7	2.7	3.1
4	1.8	2.8	3.4
5	1.9	2.9	3.4
6	2.1	3.1	3.6
7	2.3	3.2	3.9

While many of these techniques are designed to offer node verification, they can only provide end-to-end node verification using the key shared between the two nodes, meaning that only the receiver can confirm the credibility of the information on the way. This means that no advanced node can authenticate the concept in common.

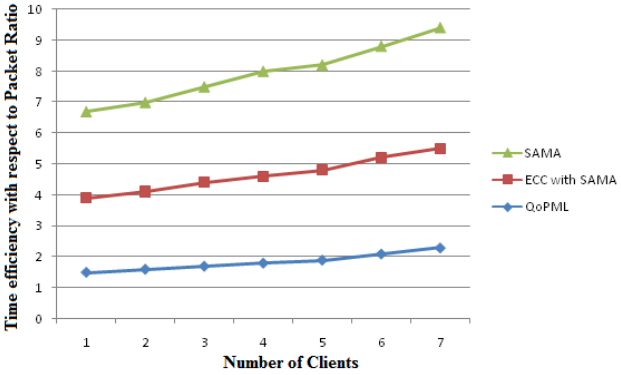

Figure-4. Time efficiency comparison results with SAMA with ECC and QoPML in communication operations.

The advanced nodes may have to ahead a controlled concept for many hops before the content can lastly be authenticated and dropped by the getting node. This not only consumes extra indicator power, but also boosts the system collision and cuts down on content distribution rate. Along with performance improvement, allowing advanced node authentication will combat opponents from performing denial-of-service strikes through concept adjustment to deplete the power and interaction sources of the wireless system. Therefore, making a method that can provide hop-by-hop advanced node verification is an important research process. In the MID protection stage method, indicator nodes are not authenticated and a malicious node can mislead indicator nodes by impersonating the Drain and delivering bogus factors P.

Table-2. Energy data values may achieved with recent configurations in application frameworks.

Scenario	Energy consumption	Life time prediction
1	43.35	299
2	68.44	185
3	75.20	170
4	260.04	48
5	413.92	31
6	376	32

Table-2 contains the power intake and life-time prediction results for the provided circumstances. The Energy intake line contains the maximal amount of power absorbed by one indicator during the execution of one scenario. The Lifetime forecast line contains the variety of days approved before battery power of any indicator is exhausted. This is prevented by the release of the receptors and parameters authentication achieved with the modified edition of the DJS method. As a result of the research, we estimate the maximum energy consumption of the node

and the life-time of the network represented as battery power level staying after given months of function. In our research study, we believe that each node has two AA battery powers with 1200mAh potential and take the maximum power intake of nodes as the energy consumption of the system for life-time forecast as shown in Table-1.

The outcomes from Table-1 display that various figures of remote detecting activities can have important impact on the lifetime of Wi-Fi indicator systems. The life-time of the first three circumstances is about 6 times longer because the number of detecting activities is similarly improved. However, the life-time of scenario variety 4 (24 unsecured sensing events) is almost twice as long as the life-time of the most properly secured scenario (number 6). The last scenario with the same variety of detecting activities for all three security levels seems to be a good bargain. The outcomes display that the developers of WSN methods should search for balance between the appropriate power intake and security level.

7. CONCLUSIONS

To provide hop-by-hop concept verification without the weakness of the built-in limit of the polynomial-based plan, we then suggested a hop-by-hop concept verification plan in accordance with the SAMA. The advanced interaction component as an extension of the QoP-ML. It is utilized to include the time and power research of interaction steps. Another participation of this paper is adding the power research and lifetime forecast segments to the QoP-ML. The results allow us to draw results about the influence of security features on time and power consumption of wireless indicator networks. Moreover, an advanced communication module is proposed as an extension of the QoP-ML language, which enhances the abilities to analyze complex wireless sensor networks.

REFERENCES

[1] Jian Li, Yun Li, Jian Ren and Jie Wu. 2014. A Hop-by-Hop Authentication and Source Privacy in Wireless Sensor Networks. IEEE transactions on parallel and distributed systems. vol. 25, no. 5, May.

[2] B. Ksiezopolski and Z. Kotulski. 2007. Adaptable security mechanism for dynamic environments. Computers and Security. 26(3): 246-255.

[3] Walid Bechkit, Yacine Challal and Abdelmadjid Bouabdallah. 2012. A New Scalable Key Pre-distribution Scheme for WSN. International Conference on Computer Communication Networks, Munich: Germany.

[4] An Liu and Peng Ning. 2008. Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks. In: Proceedings of the 7th international conference on Information processing in sensor networks, Washington, DC, USA. IEEE Computer Society. IPSN '08, pp. 245-256.

[5] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus. Tinypk. 2004. Securing sensor networks with public key technology. In: SASN 04: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, ACM Press. pp. 59-64.

[6] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantzin. 2004. Comparing elliptic curve cryptography and rsa on 8-bit cpus. CHES. pp. 119-132.

[7] J. Zhang and V. Varadharajan. 2010. Wireless sensor network key management survey and taxonomy. Journal of Network and Computer Applications. 33(2): 63-75.

[8] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones. 2010. Security in wireless sensor networks by Handbook of Information and Communication Security. pp. 513-552.

[9] P. O. Kamgueu, E. Nataf, T. Djotio, and O. Festor. 2013. Energy based metric for the routing protocol in low-power and lossy network. In: Proceedings of the 2nd International Conference on Sensor Networks (SENSORNETS 2013), pp. 145-148, Barcelona, Spain.

[10] U. Hunkeler, H. L. Truong, and A. Stanford-Clark. 2008. MQTT-S- a publish/subscribe protocol for wireless sensor networks. In: Proceedings of the 3rd IEEE/Create-Net International Conference on Communication System Software and Middleware (COMSWARE '08). pp. 791-798.

[11] T. Rault, A. Bouabdallah, and Y. Challal. 2014. Energy efficiency in wireless sensor networks: a top-down survey. Computer Networks. 67: 104-122.

[12] The ns-3 network simulator, 2008, http://www.nsnam.org/.

[13] D. Blouin and E. Senn. 2010. CAT: an extensible system level power consumption analysis toolbox for model-driven design. In: Proceedings of the 8th IEEE

International NEWCAS Conference (NEWCAS '10), pp. 33-36.

[14] J. Li, H. Y. Zhou, D.-C. Zuo, K. M. Hou, H. P. Xie, and P. Zhou. 2014. Energy consumption evaluation for wireless sensor network nodes based on queuing Petri net. International Journal of Distributed Sensor Networks. Article ID 262848, p. 11.

[15] A. K. Agarwal and W. Wang. On the impact of quality of protection in wireless local area networks with IP mobility. Mobile Networks and Applications. 12(1): 93-110.