Journal of Computer Science 9 (5): 635-645, 2013
ISSN 1549-3636
© 2013 Science Publications
doi:10.3844/jcssp.2013.635.645 Published Online 9 (5) 2013 (http://www.thescipub.com/jcs.toc)

Evaluation Metrics for Wireless Sensor Network Security: Algorithms Review and Software Tool

Qasem Abu Al-Haija, Mohamed H. Shwehdi and Muhammad Banat

Department of Electrical Engineering, King Faisal University, Al-Ahsa, 31982, P. O. Box 380, Saudi Arabia

Received 2013-03-05, Revised 2013-05-04; Accepted 2013-05-27

ABSTRACT

Wireless Sensor Networks (WSN) is currently receiving a significant attention due to their potential impact into several real life applications such as military and home automation technology. The work in this study is a complementary part of what's discussed. In this study, we propose a software tool to simulate and evaluate the six evaluation metrics presented for non-deterministic wireless sensor network in which are: Scalability, Key Connectivity, Memory complexity, Communication complexity, Power Consumption and Confidentiality. The evaluation metrics were simulated as well as evaluated to help the network designer choosing the best probabilistic security key management algorithm for certain randomly distributed sensory network.

Keywords: Wireless Sensor Networks, Evaluation Metrics, Scalability, Key Connectivity, Memory Complexity, Communication Complexity, Power Consumption, Confidentiality

I. INTRODUCTION

Wireless Sensor Networks are increasingly being used to do tasks in several environments. The technology of Wireless Sensor Networks (WSNs) (Seyit *et al*., 2005) is a hot research area in Computer Networks that expected to take a big share in the market of technology. A WSN contains hundreds to thousands of small sensors where these sensors are designed to be self-organized wireless networks. Sensor nodes have limited processing power, storage, bandwidth and energy and because of that providing security in sensor networks in not an easy task (Dong-Mei and Bing, 2006).

A sensor network is composed of a large number of nodes which are deployed densely in close proximity to the phenomenon to be monitored. Each of these nodes collects data and its purpose is to route this information back to a sink. The network must possess self-organizing capabilities since the positions of individual nodes are not predetermined. Cooperation among nodes is the dominant feature of this type of network, where groups of nodes cooperate to disseminate the information gathered in their vicinity to the user (Du *et al*., 2004).

The environment of Distributed WSN is the one of most challenging environments of the networks world, because it's an infrastructure-less network. Where the distributed WSN can be used in several environments such as military, hospitals, malls; this makes the security over distributed WSN a real challenge and more serious subject to research.

The key management approaches such as probabilistic approaches (Al-Haija, 2010; Melhem *et al*., 2009) are considered the heart of security techniques that make the use of Distributed WSN secure and reliable.

Due to no such fixed approach can be generalized to be applied over any Distributed WSN, the evaluation metrics can be computed as in (Al-Haija, 2010; Melhem *et al*., 2009) and used as a judge between all approaches.

The problem addressed in this study will focus on the probabilistic key management security approaches as well as the six evaluation metrics discussed in (Al-Haija, 2010; Melhem *et al*., 2009). The main problem is shown in **Fig. 1**.

There are different evaluation metrics that can be pplied to WSNs.

Corresponding Author: Qasem Abu Al-Haija, Department of Electrical Engineering, King Faisal University, Al-Ahsa, 31982, P.O. Box 380, Saudi Arabia

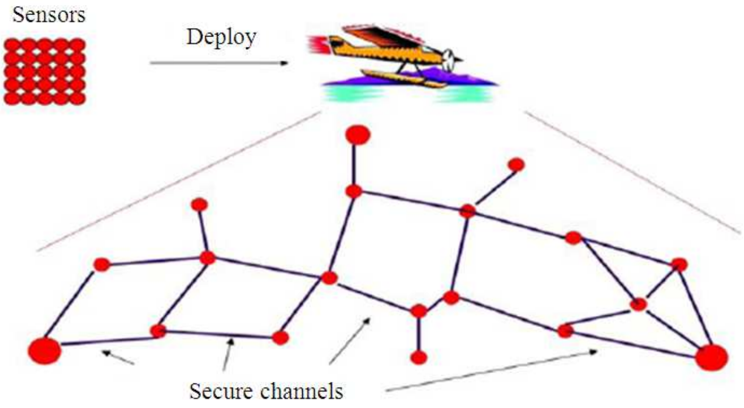


Fig. 1. Problem statement figure

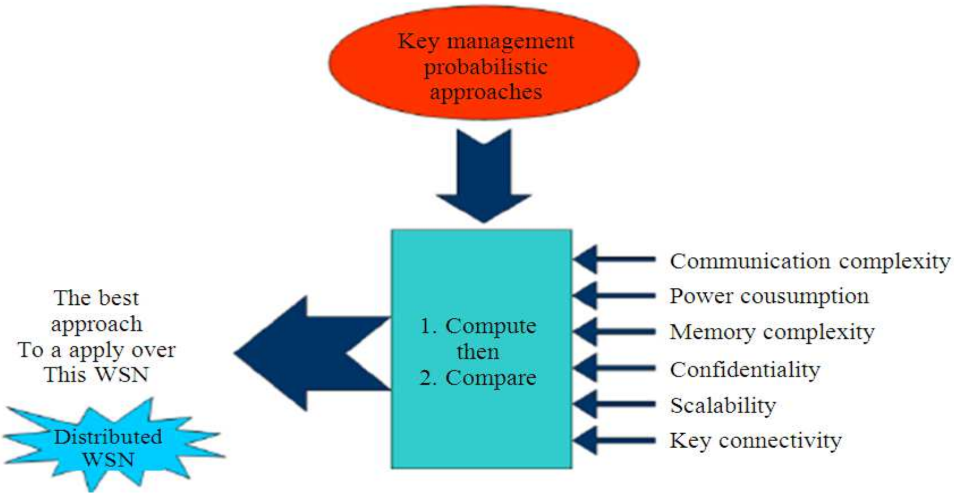


Fig. 2. Proposed simulation scheme

These evaluation metrics are important to decide which kind of nodes are going to be used in a network as well as the security scheme that can be applied for the network. The evaluation metrics used in this study are: Scalability, Key Connectivity, Memory complexity, Communication complexity, Power Consumption and Confidentiality. The proposed simulation scheme is shown in **Fig. 2**.

In this study, we propose a new software tool and algorithm to compare the different probabilistic security approaches presented in (Al-Haija, 2010) with respect to the six evaluation metrics in order to choose the best algorithm to be applied for the certain WSN. Our proposed tool will consider the system equations derived in (Al-Haija, 2010) and simulate them through VB. NET.

1.1. Related Works

In the last years, many classical solutions tried to address the key management of wireless pre-distribution security problem. The most commonly used solution is the probabilistic schemes (Xiao *et al*., 2007; Traynor *et al*., 2006; Al-Haija, 2010; Silva *et al*., 2008; Sohraby *et al*., 2007; Dong-Mei and Bing, 2006; Khalil and Ozdemir, 2012; Chan *et al*., 2003; Du *et al*., 2005; 2004; Kuchipudi and Basha, 2012).

Eschenauer and Gligor (2002) and Xiao *et al*. (2007) were the forerunner to build the first algorithm based probability using the random graph theory that is called the basic scheme, this scheme contains 3 phases: Key pre-distribution phase (where key pool generates a large number of keys P, then each node randomly selects number of keys K which called key ring), shared key discovery phase (in this phase any two nodes can establish a secure link if they shared a common key in their key rings) and, key path establishment phase (each node tries to establish a path-key with any node in their transmission range but do not share a common key with it).

Chan *et al*. (2003) proposed the Multi-path reinforcement scheme uses multiple independent paths to establish a link key. Normally, it is used with the basic scheme because this conjunction gets a good resilience against node capture attacks. The objective of this scheme is to strengthen the security of a link key. Initiation phase and key setup works like the scheme that it is in conjunction with, usually the basic scheme. This scheme tries to coordinate the key update over multiple paths. These paths can be the set of paths that are created during the initial key setup and that are disjoint. The sender node creates random values that will be routed along these different paths to the final node. When the final node receives all the keys can create the new link key like the XOR of the received keys.

Du *et al*. (2004) proposed a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. They showed that the performance (including connectivity, memory usage and network resilience against node capture) of sensor networks can be substantially improved with the use of thier proposed scheme.

Chan *et al*. (2005) used of the apriori probability to design a variant of random key predistribution method that improves the resilience and the fraction of compromised communications compared to seminal works. They related the key ring size of the subgroup node to the probability of node compromise and designed an effective scalable security mechanism that increases the resilience to the attacks for the sensor subgroups. Their simulation results showed that by using their scheme, the performance can be substantially improved in the sensor network (including the resilience and the fraction of compromised communications) that only sacrifices a small extent in the probability of a shared key exists between two nodes, compared to those of the prior results.

Traynor *et al*. (2006) considered the expenses incurred by sensor networks implementing secure routing schemes on top of probabilistic symmetric key management schemes. Specifically, they examined the overhead observed from proactive and reactive key establishment mechanisms for networks using a balanced method of key management. Through extensive simulation, they quantified more realistic costs for the application of secure hop-by-hop routing in sensor networks.

Dong-Mei and Bing (2006) investigated the constraints and special requirements of key management in sensor network environment and introduced some basic evaluation metrics. The key pre-distribution scheme is thought as the most suitable solution for key management problem in wireless sensor networks. It can be classified into four classes: pure probabilistic key predistribution, polynomial-based, Blom’s matrix-based and deterministic key pre-distribution schemes.

Xiao *et al*. (2007) have studied Random pair-wise keys scheme is a variation of the Pair-wise key scheme (Du *et al*., 2005) The main difference between both schemes is that here we use less than N-1 keys to have a connected graph with high probability. This scheme has also three phases: Initialization phase, Key setup phase and key sharing phase.

Silva *et al*. (2008) introduced a mathematical concepts and a step-by-step mathematical analysis for Key Management in Wireless Sensor Networks based on random distribution of keys among the sensor nodes. Their study led to some practical concerns about its applicability to real world applications where the technological constrains strictly compromise the mathematical theoretical models. They demonstrated that the number of communication links needed to assure near 100% network connectivity, which is considered impractical in nowadays applications.

Al-Haija (2010) in, has retrieved the four probabilistic key management approaches that have been widely used in WSNs. These approaches are: Random key predistribution, Q-composite key scheme, MultiPath Reinforcement Scheme and Random Pairwise Keys Scheme. He also provided a probabilistic analytical evaluation model to asses these protocols individually. The model comprises several factors that should be considered carefully before deploying the WSN. These factors are: scalability, confidentiality, memory complexity, communication complexity and power consumption. The results showed that the pairwise key scheme can be adapted in several diverse environment satisfying most of our study factors.

Kuchipudi and Basha (2012) proposed several key management schemes that either cannot offer strong resilience against node capture attacks, or require too much memory for achieving the desired connectivity. Their proposed Bloms algorithm outperforms others in terms of resilience against node capture. Bloms key distribution scheme with deployment knowledge provides a higher connectivity with a shorter transmission range and a lower memory requirement.

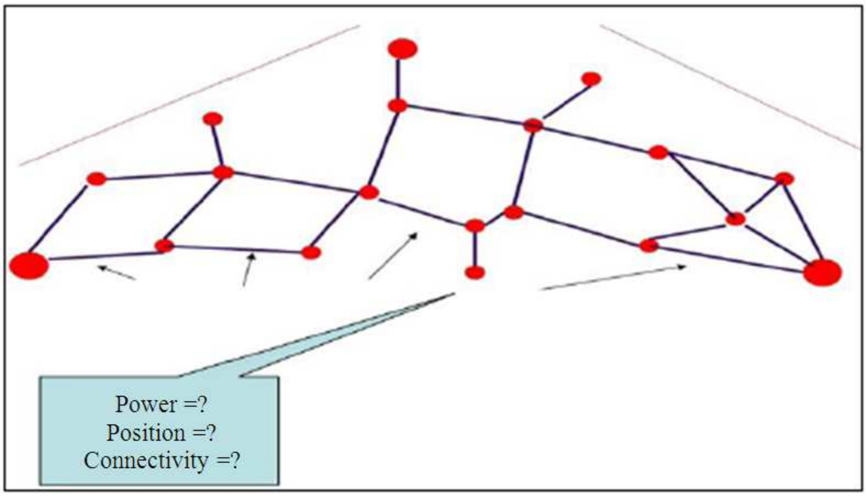


Fig. 3. Random sensors needs probabilistic methodology

They also provided an overview of different approaches of key management schemes and limitations of those approaches.

Khalil and Ozdemir (2012) evaluated the most important key management schemes in wireless sensor networks which are single network-wide key scheme, pairwise key establishment scheme, random key predistribution and Q-composite random key predistribution scheme. The evaluation is performed in OMNET++ simulation environment and the metrics are selected as secure connectivity achievement, memory overhead, communication overhead and resilience against node capture attacks. Their simulation results showed that there is no general purpose key management scheme that can fit all the security requirements of wireless sensor networks. However, in terms of the performance metrics, the most suitable scheme for wireless sensor networks is the random key predistribution scheme.

All the previous methods and other ones have a strong security for the WSN but it is static. In our approach we will try to find a solution to work as a dynamic approach based on network constraints and can determine which the best approach to apply for such WSN is.

1.2. Motivations and Methodology

The proposed research is motivated by many issues. First, the security of WSN which became very important in real life especially in critical and dangerous missions. WSN are used today in hostile environments, malls, hospitals, house appliances and armies to do different kinds of jobs, which make its security level to swing from low to high. Second, previous studies have not leaded to use such approach of key management that can be applied in any WSN. This leaded us to start thinking about some dynamic approach to use for WSN security.

The proposed methodology throughout this research consists of the following steps:

- The approach for proceeding in the proposed solution will start by finding the appropriate algorithm for solving the proposed problem. We will use the probabilistic analytical solutions discussed in (Al-Haija, 2010) to solve this problem where-as we see in **Fig. 3** is no pre-knowledge about the environment of distributed sensors
- The solution will be implemented and verified using a software simulation such as VB.NET programming language or another
- The WSN constraints will be calculated and simulated for all probabilistic security approaches according to the results and system equations discussed in (Al-Haija, 2010)

1.3. Simulation Environment

Proposed work is to design a new software tool to compare the different probabilistic security approaches presented in (Al-Haija, 2010) with respect to the six evaluation metrics (Al-Haija, 2010) in order to choose the best algorithm to be applied for the certain WSN. Our proposed solution is programmed and implemented in VB.NET programming language.

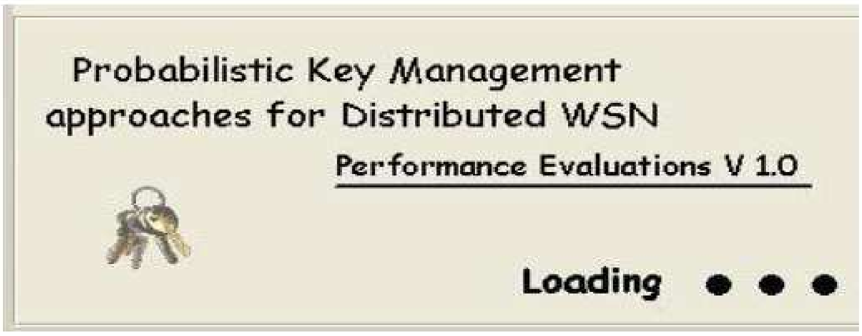

Probabilistic Key Management approaches for Distributed WSN
Performance Evaluations V 1.0
Loading ● ● ●

Fig. 4. Simulator initiating

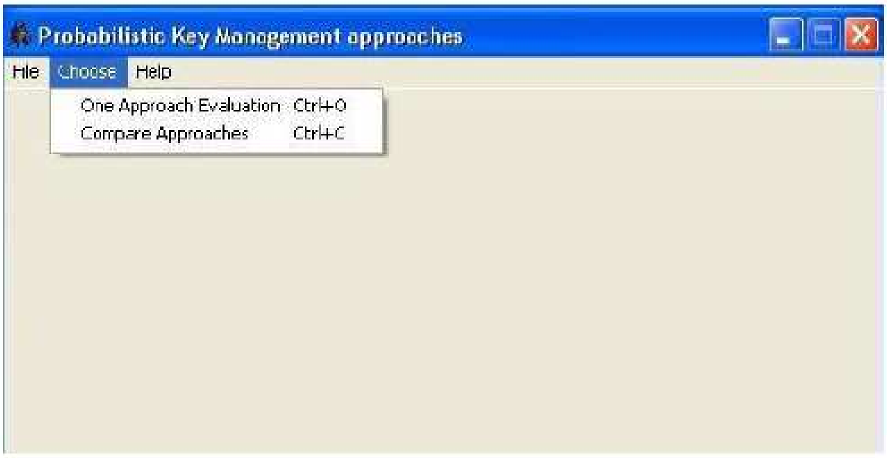

Probabilistic Key Management approaches
File
Choose
Help
One Approach Evaluation Ctrl+O
Compare Approaches Ctrl+C

Fig. 5. Choose menu

Visual Basic is a name for a new strategy: a blueprint for building applications for many decades. It's actually even more than that. It's Microsoft's commitment to remain at the top of a rapidly changing world and give us the tools to address the needs of tomorrow's computing. Visual Basic is a language for creating Windows applications, like many others. It also happens that Visual Basic is the easiest to learn, most productive language (but you already know that).

It a simple language, because it managed to hide many of the low-level details of the operating system. Those who wanted to do more with Visual Basic had to resort to Windows API.

There are many visual tools in the IDE, like the Menu Designer. This tool allows you to visually design menus and to set their names and basic properties (such as checking, enabling, or disabling certain options). Designing a menu doesn't involve any code and it's carried out with point-and click operations. Of course, you will have to insert some code behind the commands of your menus and (again) you can use any language to program them.

1.4. Tests and Results

As mentioned previously, our principle is simulated in VB. NET programming language. We have adopted two interfacing techniques to satisfy deferent requirements. The first is Command Line Interface (CLI) which is harder to use and interact but better in terms of performance. The other is the Graphical User Interface (GUI), the easier to use while worse when the performance has precedence. Anyway, we concentrate here on the GUI to show our work and results simply and clearly. **Figure 4** shows the loading interface which will be the user's start point of execution.

Here is a brief description on each component, augmented with snapshots to make everything concrete.

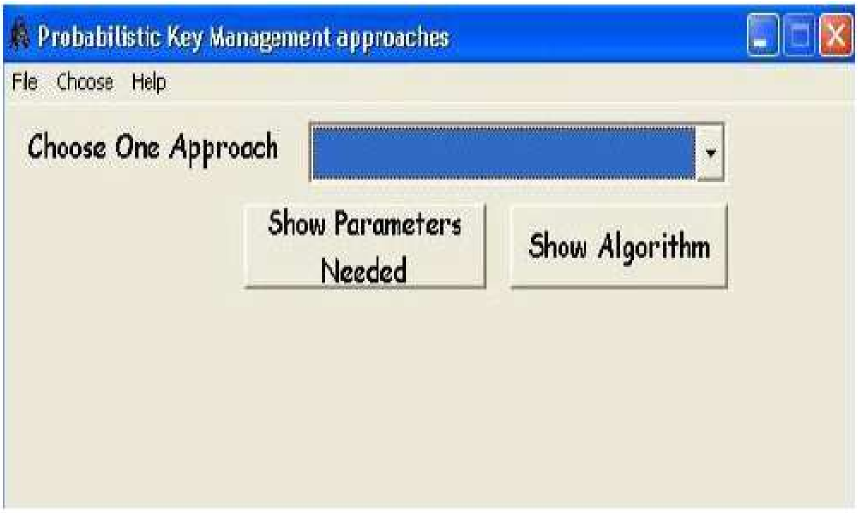


Fig. 6. One approach evaluation

The deigned simulator in **Fig. 5** defines two methods of evaluation which is placed in the menu of the first major window of simulator, those ways are: One Approach Evaluation or Compare approaches.

1.5. One Approach Evaluation

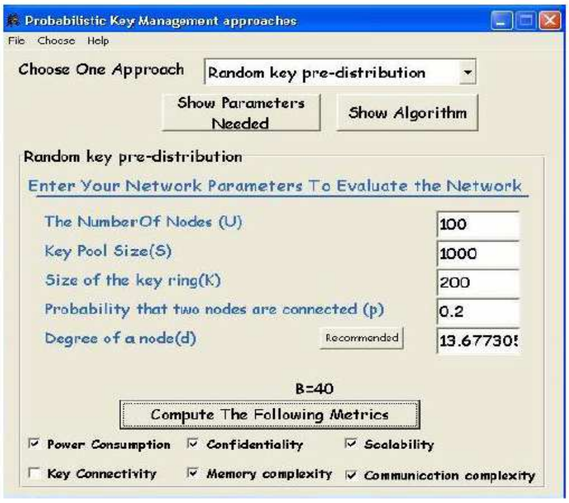
(The first major window) which allows you to test one of the four approaches then you can show all the parameters needed by that approach then you choose the required metrics to be calculated. You can use the choose menu to apply one of the four approaches which listed in combo box as shown in **Fig. 6**:

- Once you choose one approach-let's say you chose random key pre-distribution-its parameters needed to be used in the metrics calculations will be shown as in **Fig. 7**
- As you see in **Fig. 7**, now you can enter all of your network specifications to test the behavior of the selected approach from the side of some metric of the six shown metric. After entering the value of parameters and determine which metrics to be calculated, now you can use the button "Compute the following metrics" to show the results as in **Fig. 8**. Also, if you don't chose some of the metrics as "Key Connectivity" then our simulator will return 0 In that field as seen in **Fig. 8**
- Another good tool that our simulator affords it in the window of "One Approach Evaluation" is the "Show Algorithm" button which shows how the chosen approach work. Example of this tool appears in **Fig. 9**

1.6. Compare Approaches

(The Second major window) which allows you to compare the four approaches then you can show all the parameters needed by all approaches then you choose the required metrics to be calculated. We can use the choose menu to apply "compare" operation of the four approaches by using a table or by graphs as shown in **Fig. 10**:

- Compare by table: this button allows us to enter the shared parameters needed for making a comparison between the four approaches. The result of this button is shown in **Fig. 11**
- Once you chose "Compare by table" then you have to enter the shared parameters that make the comparison happen and then to use the "Compute and Compare" button. Let's assume the example in the **Fig. 12**
- Now use the "Which Best" button to achieve the goal of comparison in order to know what to use for this WSN to get the best approach that will walk with the field of WSN. The result of this example is shown in **Fig. 13**
- Compare by Drawing: another way to make a comparison is to study the behavior of each approach in the based on the metric equation graph where we used the Excel sheets as an OLE Object of the simulator drawing and specified the parameters needed in each metric as can be seen in **Fig. 14**. As you see in **Fig. 14**, the use of MDI form makes every metric to be contained as an individual form (Child Form).


Probabilistic Key Management approaches
File Choose Help
Show Parameters Needed
Show Algorithm
Recommended
Compute The Following Metrics

Choose One Approach: Random key pre-distribution

Random key pre-distribution

Enter Your Network Parameters To Evaluate the Network

The NumberOf Nodes (U): 100

Key Pool Size(S): 1000

Size of the key ring(K): 200

Probability that two nodes are connected (p): 0.2

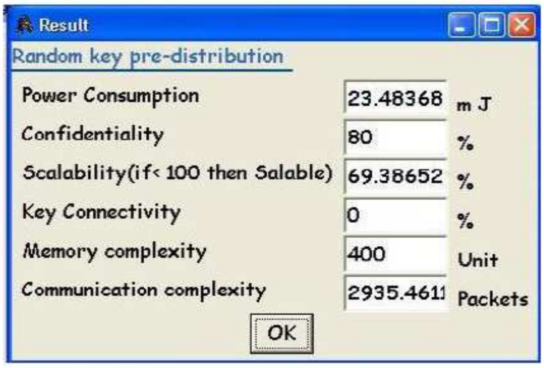
Degree of a node(d): 13.67730!

B=40

☑ Power Consumption ☑ Confidentiality ☑ Scalability

☐ Key Connectivity ☑ Memory complexity ☑ Communication complexity

Fig. 7. Random Key pre-distribution and its parameters



Random key pre-distribution

Power Consumption: 23.48368 m J

Confidentiality: 80 %

Scalability(if< 100 then Salable): 69.38652 %

Key Connectivity: 0 %

Memory complexity: 400 Unit

Communication complexity: 2935.4611 Packets

Fig. 8. Results for random key pre-distribution

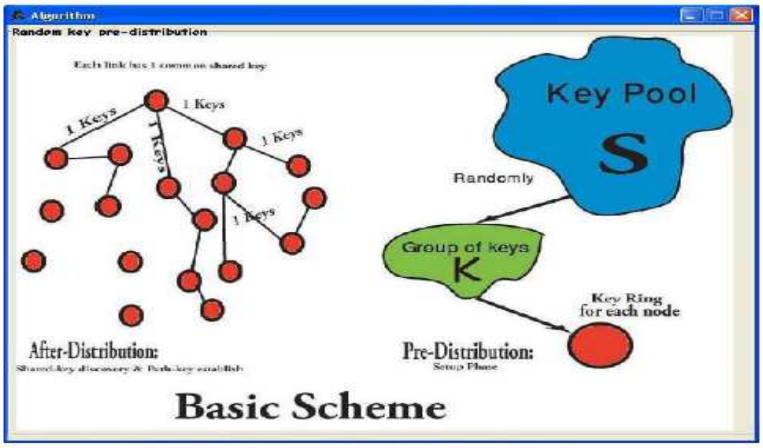


Fig. 9. Show algorithm" random key pre-distribution"

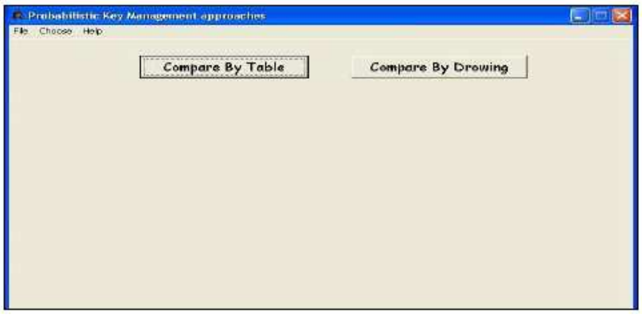


Fig. 10. Compare approaches menu

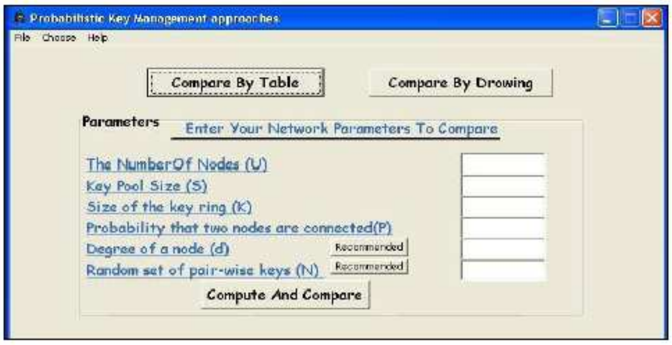
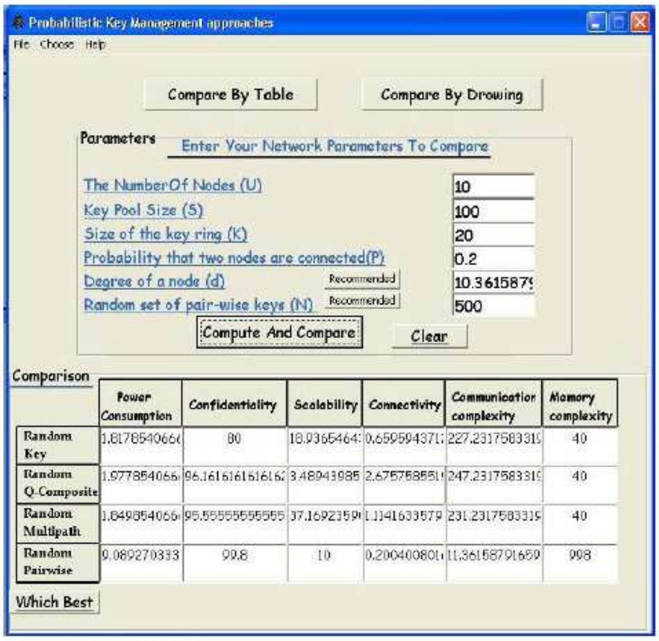


Fig. 11. Compare by table

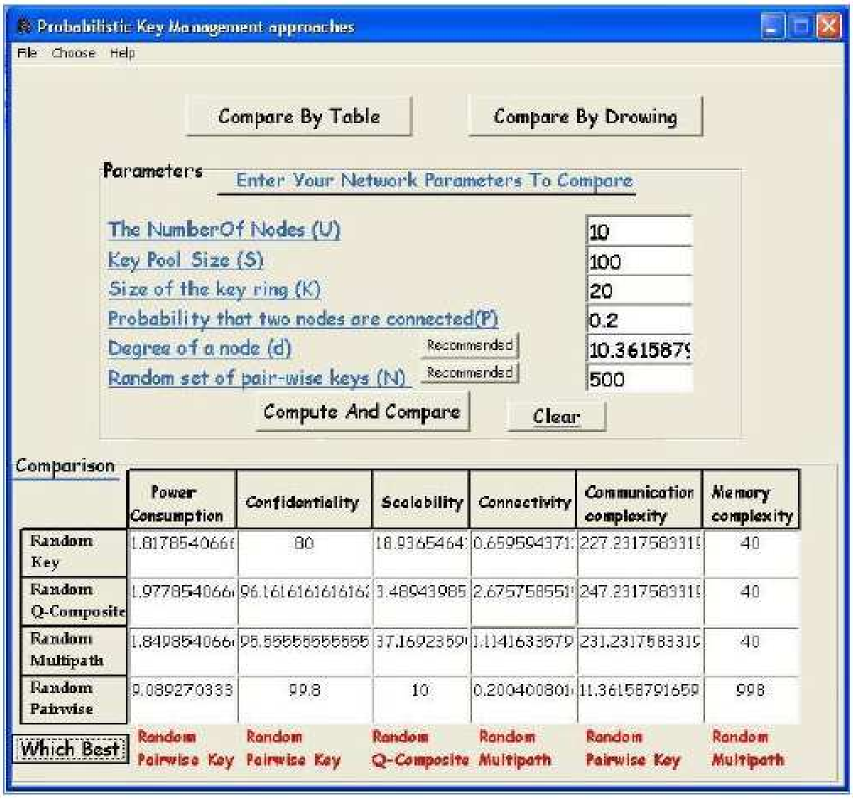


The NumberOf Nodes (U) 10
Key Pool Size (S) 100
Size of the key ring (K) 20
Probability that two nodes are connected(P) 0.2
Degree of a node (d) 10.3615879
Random set of pair-wise keys (N) 500

Comparison

	Power Consumption	Confidentiality	Scalability	Connectivity	Communication complexity	Memory complexity
Random Key	1.8178540660	80	18.9365464:	0.6595943717	227.2317583319	40
Random Q-Composite	1.977854066	96.1616161616162	3.48943985	2.675758551	247.2317583319	40
Random Multipath	1.849854066	95.5555555555	37.1692359	1.1141633579	231.2317583319	40
Random Pairwise	9.089270333	99.8	10	0.2004008010	11.36158791659	998

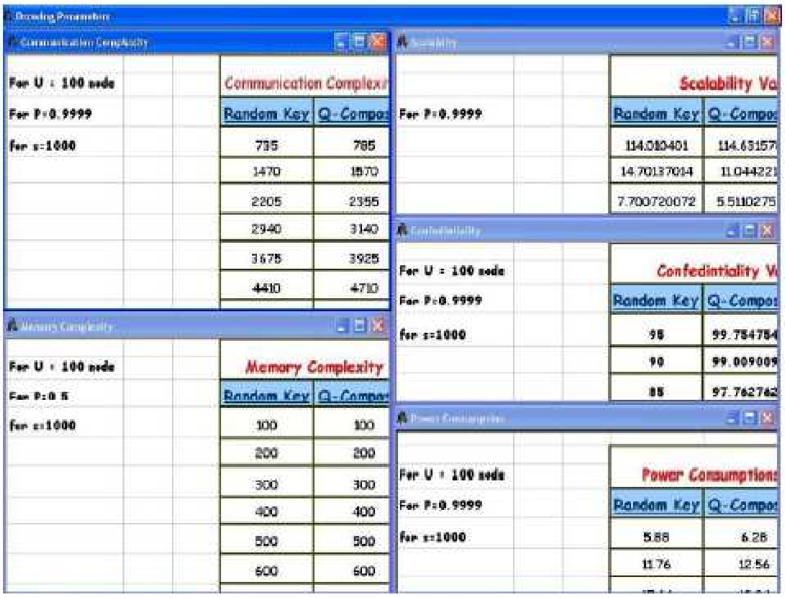
Fig. 12. The results of comparison



The NumberOf Nodes (U)	10
Key Pool Size (S)	100
Size of the key ring (K)	20
Probability that two nodes are connected(P)	0.2
Degree of a node (d)	10.3615879
Random set of pair-wise keys (N)	500

	Power Consumption	Confidentiality	Scalability	Connectivity	Communication complexity	Memory complexity
Random Key	1.8178540666	80	18.9365464	0.659594371	227.2317583319	40
Random Q-Composite	1.9778540666	96.1616161616162	3.48943985	2.67575855	247.2317583319	40
Random Multipath	1.8498540666	95.5555555555	37.16923590	1.1141633579	231.2317583319	40
Random Pairwise	9.089270333	99.8	10	0.2004008016	11.36158791659	998
Which Best	Random Pairwise Key	Random Pairwise Key	Random Q-Composite	Random Multipath	Random Pairwise Key	Random Multipath

Fig. 13. Which best bottun



For U : 100 node
For P:0.9999
for s:1000

Communication Complexi	
Random Key	Q-Compos
735	785
1470	1570
2205	2355
2940	3140
3675	3925
4410	4710

For U : 100 node
For P:0.5
for s:1000

Memory Complexity	
Random Key	Q-Compos
100	100
200	200
300	300
400	400
500	500
600	600

For P:0.9999

Scalability Va	
Random Key	Q-Compos
114.010401	114.63157
14.70137014	11.044221
7.700720072	5.5110275

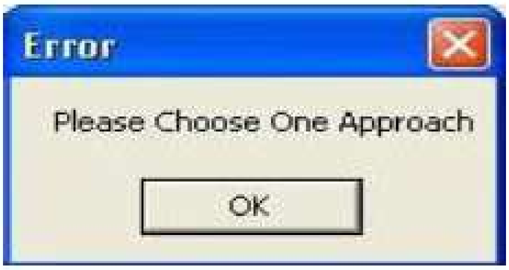
For U : 100 node
For P:0.9999
for s:1000

Confedintiality V	
Random Key	Q-Compos
98	99.754754
90	99.009009
85	97.762762

For U : 100 node
For P:0.9999
for s:1000

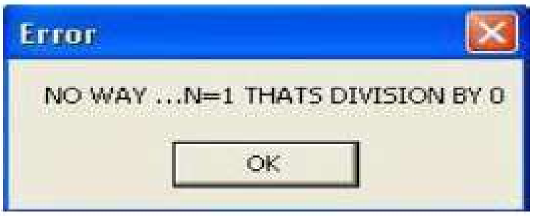
Power Consumptions	
Random Key	Q-Compos
5.88	6.28
11.76	12.56

Fig. 14. Compare by drawing


Error

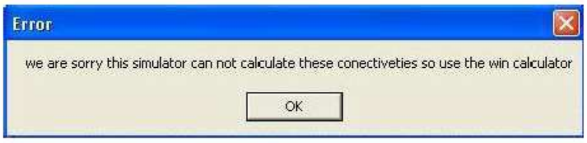
Please Choose One Approach

Fig. 15. Nothing chosen in combo box


Error

NO WAY ...N=1 THATS DIVISION BY 0

Fig. 16. Division by zero


Error

we are sorry this simulator can not calculate these conectiveties so use the win calculator

Fig. 17. Choose the value of S or K more than 170

Now you can choose one of the metrics drawing by maximize its form and the double click on the middle of it then it will behave as an excel sheet (editable to make you do your evaluations)

1.7. Some Error Messages

Figure 13-17 show some common error messages that will be generated by our simulator.

1.8. Problems and Difficulties

During the design and coding phases of the project many problems were faced on the areas of efficiency and consistency of the code. It was a good experience for me to search for design and coding solutions for such problems.

One of these problems we faced was in VB Buffer size, which is limited by the size of data type (Maximum of 16 bytes). Because we was tried to calculate the factorial function of more than 170.So we tried to solve this problem by divide the loop iterations by such number like 800 but it was not an accurate method so we left this problem to be calculated by the Windows calculator.

Dealing with probability was really a more serious issue in the understanding and the deign phases which require more focusing in the studying of probability methods phase where the probability is the most math's subjects that need more efforts to be in the right way. This problem solved by increasing the studying and researching efforts in the probability phase.

Many other problems and bugs were solved during the development of the project and many enhancements were adopted also to guarantee a good quality for the code. The problems were discovered while testing the code were either solved directly or documented and saved so that it will be solved later on.

2. CONCLUSION

A new software tools and techniques to simulate and evaluate the six evaluation metrics presented (Al-Haija, 2010) for non-deterministic wireless sensor network are implemented and proposed in this study The environment of Distributed WSN is the most challenging of the networks world, because it's an infrastructure-less network. Where the distributed WSN can be used in several environments such as military, hospitals, malls and others; that's make the security over distributed WSN a real challenge and more serious subject to research.

The key management approaches such as probabilistic approaches are considered the heart of security techniques that make the use of Distributed WSN secure and reliable.

Because no such fixed approach can be generalized to apply over any Distributed WSN, there are the evaluation metrics (e.g., Scalability, Key Connectivity, Memory complexity, Communication complexity, Power Consumption, Confidentiality) that can be computed to be the judge between all approaches. That's what we need, the best approach to be the dominator over the WSN.

This study can be modified by such methods; one of them is not just focusing on probabilistic approaches but to imply all other type of Key management approaches that can be applied over Distributed WSN such as Deterministic approaches, Hybrid approaches and Location aware schemes.

Another way to improve this study by studying another metrics such as the random mobility of Distributed WSN and include it as a metric to be calculated and simulated.

The third way is to extend the simulator capability in order of enhancing the metrics as the WSN requirements which will be done based on the nodes limitations.

3. ACKNOWLEDGEMENT

Researchers would like to thank deanship of scientific research at King Faisal University (KFU), Alhasa, Saudi Arabia for supporting this research.

4. REFERENCES

Al-Haija, Q.A., 2010. Toward secure non-deterministic distributed wireless sensor network using probabilistic key management approaches. J. Inform. Assurance Securty.

Chan, H., A. Perrig and D. Song, 2003. Random key predistribution schemes for sensor networks. Proceeding of the IEEE Symposium on Research in Security and Privacy, In Australasian Conference on Information Security, May 11-14, IEEE Explor Press, pp: 197-213. DOI: 10.1109/SECPRI.2003.1199337

Chan, S.P., R. Poovendran and M.T. Sun, 2005. A key management scheme in distributed sensor networks using attack probabilities. Proceeding of the IEEE Global Telecommunications Conference, Nov. 28-Dec. 2, IEEE Xplor Press. DOI: 10.1109/GLOCOM.2005.1577788

Dong-Mei, S. and H. Bing, 2006. Review of key management mechanisms in wireless sensor networks. ACTA Utomatica Sinica, 32: 901-906.

Du, W., J. Deng, Y. S. Han, S.Chen and P.K. Varshney, 2004. A Key management scheme for wireless sensor networks using deployment knowledge. Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies, Mar. 7-11, IEEE Xplor Press. DOI: 10.1109/INFCOM.2004.1354530

Du, W., J. Deng, Y.S. Han, P.K. Varshney, J. Katz *et al*., 2005. A pairwise key predistribution scheme for wireless sensor networks. ACM Trans. Inform. Syst. Securty, 8: 228-258. DOI: 10.1145/1065545.1065548

Eschenauer, L. and V.D. Gligor, 2002. A key-management scheme for distributed sensor networks. Proceedings of the 9th ACM Conference on Computer and Communications Security, Nov. 18-22, ACM Press, New York, USA., pp: 41-47. DOI: 10.1145/586110.586117

Khalil, O. and S. Ozdemir, 2012. Performance evaluation of key management schemes in wireless sensor networks. Gazi. Uni. J. Sci., 25: 465-476.

Kuchipudi, R. and N.M.J. Basha, 2012. A distributed nodes' localisation approach in wireless sensor networks. Int. J. Comput. Sci. Inform. Technol., 3: 3187-3190. DOI: 10.4108/ICST.MOBIQUITOUS2009.6838

Melhem, O.B., Q.A. Al-Haija and A. Al-Badawi, 2009. Performance evaluation of probabilistic key management approaches for wireless sensor networks. Proceedings of the 1st International Conference in Information and Communication Systems' (ICICS' 09).

Seyit, A., C. Amtepe and B.U. Yener, 2005. Key distribution mechanisms for wireless sensor networks: A survey. Rensselaer Polytechnic Institute-Computer Science Department Troy, New York.

Silva, R.M.S., N.S. Pereira and M.S. Nunes, 2008. Probabilistic key management practical concerns in wireless sensor networks. J. Networks, 3: 29-37. DOI: 10.4304/jnw.3.2.29-37

Sohraby, K., D. Minoli and T. Znati, 2007. Wireless Sensor Networks Technology, Protocols and Applications. 1st Edn., Wiley-Interscience, Hoboken, New Jersey, ISBN-10: 9780470112755, pp: 328.

Traynor, P. Cao, T.G. and T.L. Porta, 2006. The effects of probabilistic key management on secure routing in sensor networks. Proceedings of the IEEE Wireless Communications and Networking Conference, Apr. 3-6, IEEE Xplore Press, Las Vegas, NV., pp: 659-664. DOI: 10.1109/WCNC.2006.1683547

Xiao, Y., V.K. Rayi, B. Sun, X. Du and F. Hu *et al*., 2007. A survey of key management schemes in wireless sensor networks. Comput. Commun., 30: 2314-2341. DOI: 10.1016/j.comcom.2007.04.009