EAACK-A SECURE INTRUSION DETECTION SYSTEM FOR MANETS

[1] G.SOWJANYA,(M.Tech ,SE)
[2] K. DASARADHA RAMAIAH, M.Tech,(Ph.D), PROFESSOR & HOD, DEPARTMENT OF IT,
[3] M.NEELAKANTAPPA, M.Tech, ASSOCIATE PROFESSOR. DEPT OF IT,
[1] sowjanya.gutty@gmail.com, [3] neelakantappa.m@bvrit.ac.in,
[1, 2, 3] B.V.RAJU INSTITUTE OF TECHNOLOGY (AUTONOMOUS)– NASAPUR,

***Abstract*—As thekey distribution is the main issue in the wireless Sensor Networks data transmission due to the attacks in recent days.Basis Security services we must provide when transferring the data in Wireless Sensor Networks are authentication, access control. Sharing the key with other parties is also a main thing to consider in the network. Key Pre-Distribution is one of the most important methods in the network. In this Key Pre-Distribution method key is distributed onto the nodes before deployment. The nodes build up the network using their secret keys after deployment. That is, when they reach their destination. There are a number of aspects Wireless Sensor Networks on which key Pre-Distribution schemes are competing to achieve better results. We must concern about the security mechanisms like Cryptography,Encipherment, Digital Signature,Access Control mechanisms, Data integrity mechanisms, Authentication exchange, Traffic padding, Routing Control and Notarisation mechanisms. To achieve these mechanisms we are using key Pre-Distribution scheme. But it will lead routing overhead problems. To solve these Problems in our proposed scheme we are using an enhanced unital based key pre-Distribution scheme. With this newly proposed scheme we can solve problems and we can achieve high network scalability, good sharing portability.**

Key Terms: Wireless Sensor Networks(WSN), Key Pre-Disribution, Probablistic, Deterministic, Symmetric key.

I. Introduction

In these days the use of Wireless Sensor Networksare increased as the communication with wireless networks is increased. We can use WSNs in any circumstances like in disasters, military services and in emergency situations like floods where the wired medium is completely destroyed. But security problem is a main issue to consider in these wireless medium and we can not trust the third parties in these networks to share the key. In most cases to encrypt or decrypt a message source and destination will shares a common key called as public key. By using these common key both the end nodes will communicates easily but what in case these common key is hacked.

For these purpose we are sharing a key in advance this mechanism is called as key pre distribution scheme. In this key Pre-Distribution scheme a key distributed between the two ends in advance that is before the communication is established. But there is a problem with these scheme also that is network overheads. To solve these problem of network overheads we are proposing a new scheme called an enhanced unital based key Pre distribution scheme and with these newly proposed scheme we can achieve high network scalability and good key sharing capability. In these paper we are analysing the schemes described in the previous works that is symmetric key management and it is classified in to two cateogories that is symmetric schemes and probabilistic schemes. In these paper we are analysing our new proposed scheme unital based design scheme against the existing schemes with respect to different categories that is storage overhead, energy consumption, network scalability, secure connectivity coverage, average secure path length and network sclability and network resielence features. That will provides good overall network performances and it will shows the equal network size and reduces the problem of network overheads. In this paper we introduce the use of unital design theory in key pre-distribution for the Wireless Sensor Networks. We show that the switching from unitals to key pre-distribution gives birth to highly scalable scheme while providing low probability of sharing common keys. In this paper we are proving that our proposed scheme enhancedunital-based key pre-distribution scheme in order to network scalability and to remove network overheads at the same time it will maintains good key sharing portability and we prove that the choice of our solution parameter could guarantees high key sharing probability. In this proposed scheme that is enhanced unital design key pre distribution scheme we are using symmetric scheme this scheme is again categorised in two approaches that is probabilistic schemes and deterministic schemes. The new concept is completely depends on the key management techiniques and how we are distributing the key between the nodes is demonstrated and in the newsheme we are trying to improve the performance and networkscalability,secure connectivity coverage, average secure pathlength and network resiliency. The obtained results show that our solution enhances the network scalability while.providing good overall network

performances. Moreover, we show that at equal network size, our solution reduces significantly the storage overhead and thereby the energy consumption.The remainder of this paper is organized as follows: Section 2 presents related works on key management for WSNs. We give in Section 3 a background on unital design and we propose a basic mapping from unitals to key pre-distribution for WSNs, we analyze the main performances of the resulting scheme. In Section 4, we explain the enhanced scalable unital-based construction that we propose and we analyze its different performances. In Section 5, we compare our approach to the existing ones regarding different criteria; we give and discuss theoretical and simulation results. In Section 6, we end up this paper with some conclusions

II. RELATED WORKS: KEY MANAGEMENT SCHEMES FOR WSNS

Key predistribution is the method of distribution of keys onto nodes before deployment. Therefore, the nodes build up the network using their secret keys after deployment, that is, when they reach their target position.Keypredistribution schemes are various methods that have been developed by academicians for a better maintenance of PEA management in WSNs. Basically a key predistribution scheme has 3 phases:Keydistribution,Shared key discovery,Path-key establishment.During these phases, secret keys are generated, placed in sensor nodes, and each sensor node searches the area in its communication range to find another node to communicate. A secure link is established when two nodes discover one or more common keys (this differs in each scheme), and communication is done on that link between those two nodes. Afterwards, paths are established connecting these links, to create a connected graph. The result is a wireless communication network functioning in its own way, according to the key predistribution scheme used in creation.There are a number of aspects of WSNs on which key predistribution schemes are competing to achieve a better result. The most critical ones are: local and global connectivity, and resiliency.

A.Probabilistic schemes

In probabilistic key management schemes, each two neighboring nodes can establish a secure link with some probability If two neighboring nodes cannot establish a secure link, they establish a secure path composed of successive secure links. Eschenauer and Gligor proposed in [2] the basic Random Key Pre-distribution scheme denoted by RKP. In this scheme,
each node is pre-loaded with a key ring of k keys randomly selected from a large pool S of keys. After the deployment step, each node i exchanges with each of its neighbor j the list of key identifiers that it maintains. This allows node j to identify the keys that it shares with node i. If two neighbors share at least one key, they establish a secure link and compute
their session secret key which is one of the common keys. Otherwise, they should determine a secure path which is composed by successive secure links. The values of the key ring size k and the key pool size $|S|$ are chosen in such a way that the intersection of two key rings is not empty with a high probability. This basic approach is CPU and energy efficient but it requires a large memory space to store the key ring.
Moreover, if the network nodes are progressively corrupted, the attacker may discover a large part or the whole global key pool. Hence, a great number of links will be compromised. Chan *et al.* proposed in [3] a protocol called Q-composite scheme that enhances the resilience of RKP. In this solution,twoneighboring nodes can establish a secure link only if they share at least Q keys. The pairwise session key is calculatedas the hash of all shared keys concatenated to each other:
$Ki,j= Hash(Ks1$
$\_Ks2$
$\_...\_Ksq$
$\_$)where $Ks1,Ks2$, ...Ksq
$\_$
are the $q\_$ shared keys between the two nodes i and j ($q\_ \geq Q$).This approach enhances the resilience against node captureattacks because the attacker needs more overlap keys to breaka secure link. However, this approach degrades the networksecure connectivity coverage because neighboring nodes musthave at least Q common keys to establish a secure linkChan*et al.* proposed also in [3] a perfect secure pairwisekey pre-distribution scheme where they assign to each possiblelink between two nodes i and j a distinct key Ki,j. Prior todeployment, each node is pre-loaded with $Pc \times n$ keys, where$n$ is the network size and Pc is the desired secure coverageprobability. Since we use distinct keys to secure each pairwiselink, the resiliency against node capture is perfect and eachcaptured node does not reveal any information about externallinks. The main drawback of this scheme is the non scalabilitybecause the number of the stored keys depends linearly on thenetwork sizeDu *et al.* proposed in [4] an enhanced random scheme assumingthe node deployment knowledge. Nodes are organizedin regional groups to which are assigned different key pools,each node selects its keys from the corresponding key poolThe key pools are constructed in such a way that neighboringones share more keys than distant pools. This approach allowsto enhance the probability ofsharing common keys as wellas the resilience against node capture attacks. However, theapplication of this scheme is restrictive if the deploymentknowledge is not possibleIn [6], Liu and Ning proposed a key management scheme inwhich nodes are pre-loaded with bivariate polynomials insteadof keys. A global pool of symmetric bivariate polynomials($f(x, y) = f(y, x)$) is generated off-line and each node I is pre-loaded with a

subset of polynomials $f(i, y)$. If twoneighboring nodes share a common polynomial, the sessionkey is derived by computing the polynomial value at theneighbor identifier. This approach allows to compute distinctsecret keys which enhances the resilience against node capture.However, it requires more memory to store the polynomialsand induces more computational overhead.In [16], Blom proposed a λ-secure symmetric key generationsystem in which each node i stores a column i and a row i of size $(\lambda + 1)$ of two matrices G and $(DG)T$respectively where : $D(\lambda+1)\times(\lambda+1)$ is a symmetric matrix,$G(\lambda+1)\times n$ is a public matrix and $(DG)T$ is a secret matrix.The matrix of pairwise keys of a group of n nodes is then $K = (DG)TG$. Yu and Guan [7] used the Blom's scheme for key pre-distribution in group-based WSNs. Nodes are deployed into a grid and to each group is assigned a distinct secret matrix. Using deployment knowledge, the potential number of neighboring nodes decreases which requires less memory. The application of this solution gives good results in the case of node deployment knowledge which is not always possible In [8], Ruj*et al.* propose a trade-based key management scheme denoted Trade-KP. Given a finite set X of v elements, an *Steiner trade* $t - (v, k)$ is defined to be two *disjoint* sets $T1$ and $T2$ of k-elements blocks of X such that each set of t elements from X occurs in precisely the same number of blocks of $T1$ as those of $T2$, and no set of t elements from X is repeated more than once in any of $T1$ or $T2$. An Steiner trade is said to be strong if any two blocks of $T1$ and $T2$ respectively intersects in at most two elements. Ruj*et al.* proposed a new trade construction: Having q a prime power and k $(4 \leq k < q)$, they construct $T1$ and $T2$ while the blocks of $T1$ are represented by $t1i,j= \{(x, (xi + j) \bmod q) : 0 \leq x < k\}$ where $0 \leq i, j < q$, and the blocks of $T2$ are represented by $t2\ i,j=\_(x, (x2 + xi + j) \bmod q) : 0 \leq x < k\ \_$, where $0 \leq i, j < q$. Ruj*et al.* proved that the proposed construction results in a $2 - (qk, k)$ strong Steiner trade. They proposed then a mapping to key pre-distribution where they associate to each element a distinct key and to each block of $T1$ and $T2$ a key ring. The key ring size is then equal to k and the scalability of the scheme is equal to $2q2$ After the deployment step, each two nodes can establish a direct secure link if they share exactly two common keys which are used to compute the pairwise session key. Based on the trade properties, authors prove that each pair of keysoccurs either in exactly two nodes from $T1$ and $T2$ respectively or none of the nodes.The main strength of the proposed scheme is the establishmentof unique secret pairwise keys between connected nodes.However, this does not ensure a perfect network resilience as we prove later. Indeed, the attacker may construct a part of the global set of keys and then compute pairwise secret keys used to secure external links where the compromised nodes are not involved. Moreover, the proposed scheme provides a low session key sharing probability which does not exceed 0.25 as we show later. *B. Deterministic schemes* Deterministic schemes ensure that each node is able to establish a pair-wise key with all its neighbors. Many solutions were proposed to guarantee determinism.A naive deterministic key pre-distribution scheme can be designed by assigning to each link (i,j) a distinct key $Ki,j$and pre-loading each node with $(n - 1)$ pairwise keys in which itis involved where n is the network size. It is obvious that this solution is not scalable for large WSNs. Choi *et al.* proposed in [17] an enhanced approach allowing to store only $(n+1)/2$ keys at each node. For that purpose, they propose to establish an order relation between node identifiers and propose a hash
function based key establishment in order to store only half of the node symmetric keys while computing the other half at each node. This approach allows to reduce the required stored keys to the half of network size, however, it is obvious that this scheme remains non scalable enough.LEAP [9] make use of a common transitory key which is preloaded into all nodes prior to deployment of the WSN. The
transitory key is used to generate pairwise session keys and is cleared from the memory of nodes by the end of a short time interval after their deployment. LEAP is based on the assumption that a sensor node, after its deployment, is secure during a time $Tmin$and cannot be compromised during this period of time. LEAP is then secure as far as this assumption is verified.In [10], C¸ amtepe and Yener proposed to use combinatorial design for key pre-distribution in WSN. They proposed a new deterministic key pre-distribution scheme based on Symmetric Balanced Incomplete Block Design (SBIBD). The proposed mapping from SBIBD to key pre-distribution allows
to construct $m2 + m + 1$ key rings from a key pool S of $m2 + m+1$ keys such that each key ring contains $k = m+1$ keys and each two key rings shares exactly one common key. The main strength of the C¸ amtepe scheme is the total

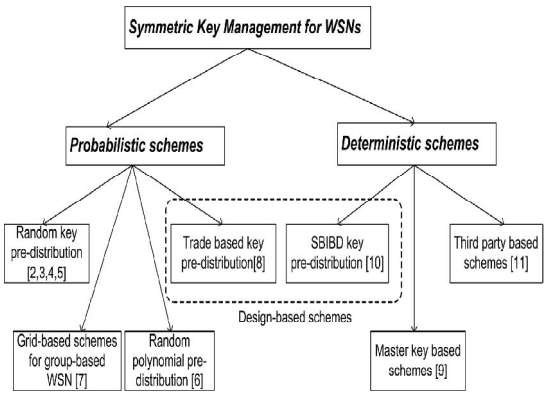

Fig. 1. Classification of symmetric key management schemes for WSNs

secure connectivity, indeed each two nodes share exactly one common key. However, the SBIBD scheme does not scale to very large networks. Indeed, using key rings of $m+1$ keys we can generate only $m2 + m + 1$ key rings. SBIBD based key pre-distribution was also used in [18] to

guarantee intra-region secure communications in grid group WSNs.

In this work, we seek to design a scalable key managementscheme which ensures a good secure coverage of large scalenetworks with a low key storage overhead. Basic schemesgiving a perfect network resilience [3] [17] achieve a networkscalability of $O(k)$ where k is the key ring size. The SBIBD[10] and the trade [8] based ones allow to achieve a networkscalability of $O(k2)$. In this work, we propose new solutionsachieving a network scalability up to $O(k4)$ when providinghigh secure connectivity coverage and good overall performances.For this purpose, we make use of the unital designtheory in order to pre-distribute keys. We propose in whatfollows a basic mapping from unitals to key pre-distributionas well as an enhanced unital based scheme which achieves agood trade-off between scalability and connectivity.

III. UNITAL DESIGN FOR KEY PRE-DISTRIBUTION INWSNS

WSNs are highly resource constrained. In particular, theysuffer from reduced storage capacity. Therefore, it is essentialto design smart techniques to build blocks of keys that willbe embedded on the nodes to secure the network links.Nonetheless, in most existing solutions, the design of key rings(blocks of keys) is strongly related to the network size, these
solutions either suffer from low scalability, or degrade otherperformance metrics including secure connectivity and storageoverhead. This motivates the use of unital design theory thatallows a smart building of blocks with unique features thatallow to cope with the scalability and connectivity issues.

In what follows, we start by providing the definition andthe features of unital design theory. We explain then thebasic mapping from unital to key pre-distribution and evaluateits performance metrics. We propose finally an enhancedunital-based scheme which achieves a good trade-off between scalability and connectivity.

A.Background: Unital Design

In combinatorics, the design theory deals with the existenceand construction of systems of finite sets whose intersectionshave specified numerical properties. Formally, A t-design(v,b,r,k,λ)is defined as follows : Given a finite setXofvpoints (elements), we construct a family ofbsubsets ofX, called blocks, such that each block has a sizek, eachpoint is contained inrblocks and eachtpoints are containedtogether in exactlyλblocks.

IV. A NEWSCALABLEUNITAL-BASEDKEYPRE-DISTRIBUTIONSCHEME FORWSNS

In this section, we present a new unital-based key pre-distribution scheme for WSNs. In order to enhance the keysharing probability while maintaining high network scalability,we propose to build the unital design blocks and pre-load eachnode with a number of blocks picked in a selective way
.

A.Key Pre-distribution

Before the deployment step, we generate blocks ofmorderunital design, where each block corresponds to a key set. Wepre-load then each node with completely disjointblockswheretis a protocol parameter thatwe will discuss later in this
section. In lemma 1, we demonstrate the condition of existenceof suchcompletely disjoint blocks among the unitalblocks.In the basic approach each node is pre-loaded with only oneunital block and we proved that each two nodes share at mostone key. Contrary to this, pre-loading each two nodes withdisjoint unital blocks means that each two nodes share betweenzero andkeys since each two unitals blocks share at mostone element.

After the deployment step, each two neighbors exchangethe identifiers of their keys in order to determine the commonkeys. If two neighboring nodes share one or more keys,we propose to compute the pairwise secret key as the hashof all their common keys concatenated to each other. Theused hash function may beSHA-1[22] for instance. Thisapproach enhances the network resiliency since the attackerhave to compromise more overlap keys to break a secure link.Otherwise, when neighbors do not share any key, they shouldfind a secure path composed of successive secure links.The major advantage of this approach is the improvementof the key sharing probability. As we will prove in nextsubsection, this approach allows to achieve a high secureconnectivity coverage since each node is pre-loaded withdisjoint blocks. Moreover, this approach gives good networkresiliencythrough the composite pairwise secret keys whichreinforces secure links. In addition, we show that our solutionmaintains a high network scalability compared to existing

V. PERFORMANCE COMPARISON

In this section, we compare the proposed unital-basedschemes to existing schemes regarding different criteria (werecall that metric definitions are given in table

A. Network scalability at equal key ring size

We compare in Figure 3 the scalability of the proposedunital based schemes against that of the SBIBD-KP and theTrade-KP ones. The network scalability of the t-UKP schemesis computed as the averagevalue between the maximumand the minimum scalability.

The network scalability of theSBIBD-KP scheme is computed asm2+m+1wheremis the SBIBD design order andm+1is the key ring size.We compute the salability of the Trade-KP scheme as2q2whereqis the first prime power greater than the key ring sizek, this value allows a achieve the best session key sharingprobability using the Trade-KP scheme as we proved in [13].The figure shows that at equal key ring size, the NU-KPscheme allows to enhance greatly the scalability comparedto the other schemes; for instance theincrease factor reaches10000compared to the SBIBD-KP scheme when the key ringsize exceeds 100. Moreover, the figure shows that the t-UKPschemes achieve a high network scalability. We notice that thehighertis, the lower network scalability is. Nevertheless, 2-UKP and 3-UKP give better results than those of the SBIBD-KP

We proposed, in this work, a scalable key management scheme which ensures a good secure coverage of large scale WSN with a low key storage overhead and a good network re-siliency. We make use of the unital design theory. We showed that a basic mapping from unitals to key pre-distribution allows to achieve high network scalability while giving a low direct secure connectivity coverage. We proposed then an efficient scalable unital-based key pre-distribution scheme pro-and the Trade-KP solutions. Even we chooset=√mas we propose (UKP*), the network scalability is enhanced.For instance, compared to SBIBD-KP scheme, the increasefactor reaches five when the key ring size equal to 150. Weplot in Figure 4 the same results separately with linear scaleswhich illustrate clearly the network scalability enhancementwhen using our solutions.

The authors of [3], assess the network scalability of ran-dom schemes including the RKP and the Q-composite onesregarding to the desired network connectivity and to the net-work capacity to maintain secure links while some nodes arecompromised. They defined for that a thresholdfmcalled thelimited global payoff requirement.The later can be explainedas the level of compromise past where the adversary gains anunacceptably information on the other pairwise secret keys.Depending onPcandfmthey defined the maximum numbersupported network size. The authors of [3] present results for

Pc=0.33andfm=0.1and show that the network scalability with a key ring size of 100 is about 300 for RKP scheme and between 600 and 700 when using Q-composite schemes. The scalability of the same schemes with a key ring size of 400 is respectively of about 1200 and between 2700 and 2800.We can see clearly that our solutions allow to reach much better network scalability than the random schemes under the suggested parameters.

B. Key ring size at equal network size

In this subsection, we compare the required key ring size when using the unital-based, the SBIBD-KP and the Trade-KP schemes at equal network size. We compute for each network size the design order allowing to achieve the desired scalability and we deduce then the key ring size, the obtainedresults are reported in Figure 5. The figure shows that at equal network size, the NU-KP scheme allows to reduce the key ring size and then the storage overhead. Indeed the enhancement factor over the SBIBD-KP scheme reaches 20. When using the t-UKP schemes, the results show that the higher t is,the higher required key ring size is. However, this value remains significantly lower than the required key ring size of the SBIBD-KP and the Trade-KP schemes. Moreover, we can see clearly in the figure, that at equal network size, the UKP* scheme provides very good key ring size compared the SBIBD-KP and the Trade-KP schemes. For instance, the key ring size may be reduced over a factor greater than two when using the UKP* compared to the SBIBD-KP scheme.

C. Energy consumption at equal network size

In this subsection, we compare the energy consumptioninduced by the direct secure link establishment phase. Sinceeach node broadcasts its list of key identifiers to its neighbors,the energy consumption can be computed as :E=Etx·klog2(S)+η·Erxklog2(|S|)whereEtx(resp.Erx) is the average energy consumed bythe transmission (resp. reception) of one bit,kis the keyring size,ηis the average number of neighbors andlog2(S|)represents the size of a key identifier in bits that we round upto the nearest byte size.We compare the energy consumption of our solutionsagainst SBIBD-KP and Trade-KP. The results plotted in Fig-ure 6 show that at equal network size, the NU-KP schemeconsumes very small amount of energy to exchange the lownumber of key identifiers. We also note that the highertis, thehigher the consumed energy is. This is due to the increasednumber of stored keys and thereby the increased number ofexchanged identifiers. Finally, the figure shows clearly thatUKP* scheme consumes less energy than the SBIBD-KP andthe Trade-KP schemes. This matches our expectation sincethe energy consumption is strongly correlated to the numberof stored keys.

D. Network connectivity at equal key ring size

We compare in this subsection, the network secure con-nectivity coverage of the different schemes. First, we plotin Figure 7 (a) the key sharing probability when using theunital based schemes (NU-KP, t-UKP and UKP*). The figureshows that the NU-KP scheme provides a bad direct secureconnectivity coverage which decreases significantly when thekey ring size increases. Indeed, the key sharing probabilityis low and tends toO(1k)asktends to infinity. Otherwise,the obtained results show that the highertis, the betterthe direct secure connectivity coverage is. Indeed,

loadingnodes with many blocks from unital design allows to increasesignificantly the key sharing probability. The figure showsmoreover that the UKP* scheme gives very good connectivityresults. For instance, the direct secure connectivity coverageremains between 0.82 and 0.66 when the key ring size isbetween 10 and 150. As the key ring size is high, the directsecure connectivity of UKP* approaches1 – e – 1≈0.632
which we proved to be an approximate lower bound.

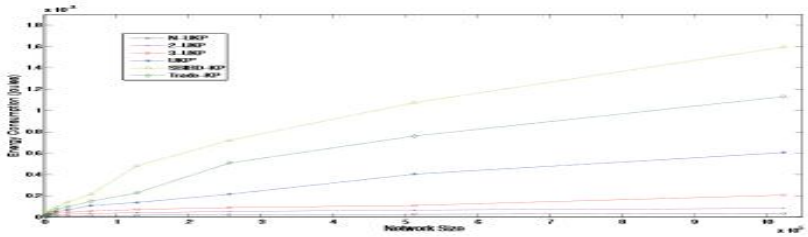

Fig. 6. Energy consumption at equal network size: we consider a grid deployment model [23] where η (the average node degree) is set to $4\log(n)$ (n is the network size). The latter value ensures the physical network connectivity and coverage [23]. $\mathcal{E}_{tx}$ and $\mathcal{E}_{rx}$ are set to the values of CC1000 radio configuration, i.e. 1625 nJ and 1156 nJ resp. [24].

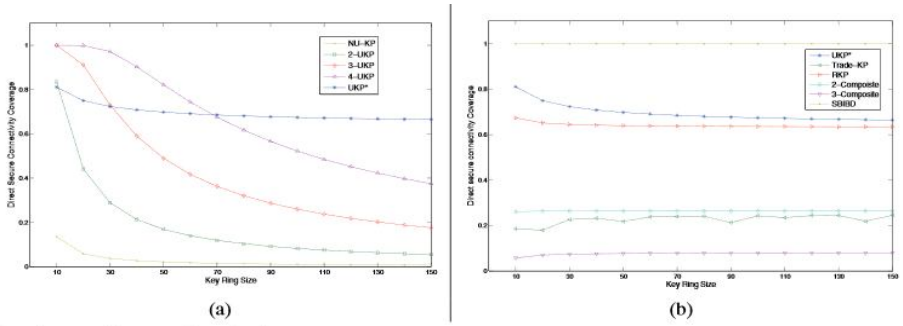

Fig. 7. Network connectivity at equal key ring size.

E. Numerical results

We provide in table IV numerical results comparing networkscalability, direct secure connectivity coverage, and averagesecure path length of the three schemes (SBIBD-KP, Trade-KPand UKP*) at equal key ring size. We notice that we providethe average network scalability (number of nodes) when usingUKP* scheme. On the other hand, we compute the averagesecure path length based on simulations. We refer in thesesimulations to the results given in [23] in order to constructa grid deployment model which ensures the network physicalconnectivity and coverage. Numerical results show that theunital-based key pre-distribution scheme UKP* increases thenetwork scalability over the SBIBD-KP and the Trade-KPscheme while maintaining high secure connectivity coverage.For instance, the network maximum size is increased by afactor of 3 and 4.8 when the key ring size is equal to 68and 140 respectively compared to the SBIBD-KP scheme. Inaddition, we maintain a high connectivity over 0.63 whichensures a low average secure path length which does notexceed 1.37.

VI. CONCLUSION

Providing high network scalability and good secure connectivity coverage. We discuss the solution parameter and we propose adequate values giving a very good trade-off between network scalability and secure connectivity. We conducted analytical analysis and simulations to compare our new solution to existing ones, the results showed that our approach ensures a high secure coverage of large scale networks while providing good overall performances.

REFERENCES

[1] Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: a survey,” IEEE Commun. Surv.Tuts., vol. 10, no. 1–4, pp. 6–28, 2008.

[2] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in Proc. 2002 ACM CCS , pp. 41–47.

[3] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes forsensornetworks,"in IEEE SP, pp. 197–213, 2003.

[4] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in
Proc. 2004 IEEE INFOCOM , pp. 586–597.

[5] C. Castelluccia and A. Spognardi, "A robust key pre-distribution pro-tocol for multi-phase wireless sensor networks," in Proc. 2007 IEEE Securecom
, pp. 351–360.