Study of the effects of pairwise key pre-distribution scheme on the performance of a Topology Control Protocol

Mohamed Mostafa M. Fouad[1], Ahmed Reda Dawood[2], Mostafa-Sami M. Mostafa[3]

[1]Arab Academy for Science, Technology, and Maritime Transport, Cairo, Egypt
Email: mmostafa_fouad@yahoo.com, mohamed_mostafa@aast.edu
[2]Arab Academy for Science, Technology, and Maritime Transport, Cairo, Egypt
Email: ahmedredadawood@gmail.com, dawood@aast.edu
[3]Faculty of Computers and Information, Helwan University, Cairo, Egypt
Email: mostafa.sami@fci.helwan.edu.eg

***Abstract*—Collecting information from open and possibly hostile environments makes the wireless Sensor Network (WSN) vulnerable to different types of security threats [1]. To provide secure communications for the WSNs, all messages have to be encrypted with a secret key. Message encryption using the public key cryptosystems [2] in WSN is not applicable due to sensor's constrained resources. A random key pre-distribution scheme and its enhanced versions to deal with pairwise key establishment [3] are of popular approaches that have higher resilience for nodes compromising. On the other hand, the topology control protocols are special forms of WSNs that add some constraints for controlling the construction of wireless networks. This paper aims to identify whether it is applicable to apply a key pre-distribution technique on a topology control protocol and evaluates its performance.**

***Keywords*-Wireless Sensor Network (WSN); key pre-distribution; Topology control protocol.**

I. INTRODUCTION

In recent years, WSNs have attracted much attention due to its great potential to be used in various real life applications. A WSN consists from hundreds to thousands of low cost sensor nodes which could either have a fixed location or randomly deployed to monitor the environment. Due to their small size, they have a number of limitations; as a limited radio bandwidth transceiver for communication, a small amount of memory and storage space for the code, and small un-chargeable batteries as an energy source. These sensor nodes are communicating in an ad-hoc manner and collaborate to collect information form their environment [4].

Providing secure, authenticated, and encrypted communication channels between sensor nodes is particularly challenging in sensor networks on account of the resource limitations of sensor nodes. The open problem is how to set up the secret keys between communicating nodes. This problem is known as the key agreement problem [5]. Although many solution schemes had been proposed, some of them are not applicable since the sensor node is typically powered by limited lifetime batteries and has a limited computational capabilities. Asymmetric cryptosystems approaches such as Diffie-Hellman key agreement [6] or RSA [7], are infeasible on the basis of constrained resources of these sensor nodes as mentioned in [8]. The key pre-deployment approaches had been proved as recommended approaches used by WSN in which a setup server assigned for each sensor node a subset of randomly selected keys from a large pool of keys [3], [9]. After nodes deployment, if two sensor nodes are within communication range of each other and share at least one common key, they can establish a secure channel using this common key(s). The main advantage of using such approach is its resilience against node capture attacks; that guarantees reliability of a network even if some of its nodes had revealed their keys.

The paper surveys the feasibility to apply a key pre-distribution technique on a topology control protocol like the A3 protocol [10]. The evaluation metric tests the topology's characteristics changed as the number of active nodes, the amount of consumed energy in constructing a reduced topology.

This paper is organized as follows. In Section 2, an introduction to topology control techniques and a detailed description of the A3 topology construction protocol. Section 3, defines briefly the key pre-distribution techniques. Section 4, introduces the methodology and simulation results. Finally Section 5, represents the conclusions.

II. TOPOLOGY CONTROL PROTOCOLS

Topology control protocols are of the most known techniques that extend the lifetime of the wireless sensor network [11], [12], [13] via reducing the number of active nodes and active links with insurance of connectivity and coverage characteristics of the network. Figure 1 [13] illustrates the algorithm of a typical topology control protocol; that once the initial topology has been established, the topology control algorithm performs two iterative phases: the *topology construction phase* and the *topology maintenance phase*. The objective of topology construction phase is to reduce

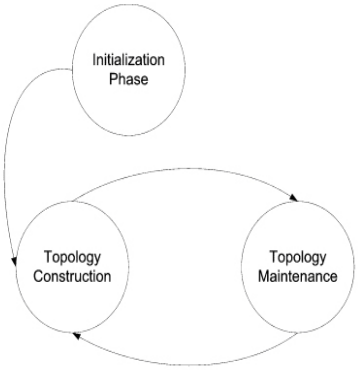


Figure 1 The topology control phases.

that initial topology by turning unnecessary nodes off and adopting the optimal transmission power of sensor nodes.

Transmit power control is a highly effective technique for minimizing interference and energy consumption in wireless networks. It was early proposed in [14], [15]. It aims to enforce the packet to go through multi-hops with an assigned lower transmission power rather than a long direct transmission which consumes a great amount of power. Another feature of this transmission control is reducing packets collision which, in turn, saves energy by reducing the power needed for packets retransmission in collision situations.

Once the reduced topology has been constructed, the network starts gathering information from its environment. Every active node participating in the reduced topology carries out many activities that drain its energy-these activities include: sensing, processing, and distribution of sensed data. Therefore, in order to extend the network's lifetime, a topology maintenance phase monitors the network status and takes the decision for switching to a new topology construction phase. The decisions are taken according to certain triggering criteria [13], [16] such as node's failure, a specific energy threshold, or a pre-defined fixed time expiry.

The topology maintenance phase gives opportunities for every node to participate in the network. It is gradually waking up some of the sleeping nodes to take the lead from the currently exhausted active one. Topology maintenance techniques are categorized as static, or dynamic. The static topology maintenance techniques build and save all the future possible communication scenarios in the first phase of constructing the first reduced topology. Static Global Time-based Topology Rotation (SGTTRot) and Static Global Energy-based Topology Rotation (SGETRot) are examples of the static topology maintenance techniques [13]. Contrary to static topologies, the dynamic topology maintenance techniques, whenever triggering criteria exist, initiate a new reduced constructing topology from scratch. Dynamic Global Time-based Topology Recreation (DGTTRec) and Dynamic Global Energy-based Topology Recreation (DGETRec) are examples of the dynamic topology maintenance techniques [13].

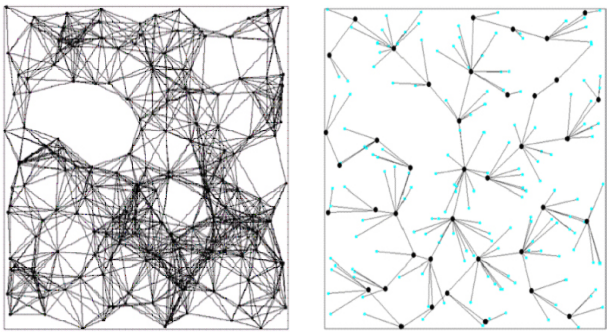
A number of disadvantages are associated with static techniques. First, they need a large memory space in order to save all the future constructing topologies. Second, they may ignore any new future added nodes. Finally, and most importantly, they consume more time and energy by virtue of running the topology construction process several times. Nevertheless, dynamic techniques are more practical to be used since they consider the current status of the network when initiating a new topology construction process so they usually choose an optimal or close to optimal topology every time it is run, resulting in better or more adequate subsequent topologies, as compared with static techniques [13].

A. THE A3 PROTOCOL

The A3 protocol [10], [13] is a topology construction protocol based on the growing tree technique [17] which defines a backbone of Connected Dominating Set (CDS) [18] of active nodes and turns other nodes off. The A3 algorithm assumes no prior knowledge about the position or orientation of the nodes. The algorithm uses messages to determine the neighbor's distance and their energy level based on the strength of those sent and received messages. These calculated energy and distance characteristics are saved by each node as its selection metric. The used messages are categorized into four types: *Hello Message*, *Parent Recognition Message*, *Children Recognition Message*, and *Sleep Message*. The following steps briefly describe the A3 algorithm:

1) A parent node (initially, the sink node) sends a *Hello Message* to its neighbors..
2) These neighbors-in the transmission range that receive that message-check their status whether they are not covered yet (i.e., have no parent) and answer back with their IDs and their selection metrics in a *Parent Recognition Message*; otherwise, they ignore the *Hello Message*.
3) After a predefined time expiry, the parent node sends back a *Children Recognition Message* to its children including a list of candidate nodes that could join the CDS. The candidates list is sorted according to the selection metrics of those candidates.
4) The best elected candidate sends a *Sleeping Message* request for its brothers to turn themselves off.
5) The best candidate starts its own neighborhood discovery process by sending a new *Hello Message*.
6) This process iterates until all network's nodes get a final status either an Active status (belong to the backbone tree) or a Sleep status (turned off).

Figure 2 [19] shows an example of a fully connected network of 200 nodes and another reduced topology using A3 algorithm, that selected 40 out of 200 nodes to be active.



(a) Original topology (b) Reduced topology with A3

Figure 2 An example of reducing original topology using A3.

The messages flood in the A3 protocol between parent nodes and their children have a low complexity of *O(N)*, bounded by *4N*, where *N* is the number of nodes in the network. In addition the A3 has computational complexity of *O(N Log N)* due to the sorting algorithms executed by every node [19].

Because the A3 protocol doesn't need prior knowledge about location and depends simply on messaging between nodes it proved that it is very scalable. Using a low cost energy and linearly bounded messages, the A3 protocol proved that it is a very energy efficient protocol that can be called iteratively in the topology control cycle.

III. RELATED WORK

A. THE PAIRWISE KEY ESTABLISHMENT TECHNIQUES

Key pre-distribution techniques allow sensor nodes to communicate securely with each other using encrypted messages. The main idea behind the pairwise key establishment process is assigning for each node a random subset of keys from a large pool of keys prior deployment. After the deployment, each pair of nodes tries to find one common key within their subsets and use that key as their shared secret key. One of the simplest solutions to do that is applying the Fully Pairwise Scheme, in which every node shares a unique key with every other node in the network. i.e., for a network of *N* nodes, each node stores *N-1* keys. As a result the total number of keys used by every node in the network is *N(N-1)/2*. The resilience of this scheme is perfect because a compromised node only reveals *N-1* link keys (from the total of *N(N-1)/2* keys). It will not reveal information about other current communications in other parts of the network. However, the amount of storage requirement by each node increases linearly with the size of the network. Thus this scheme is impractical for sensors with an extremely limited amount of memory.

To minimize the memory usage by each node, Eschenauer and Gligor [20] proposed a probabilistic key pre-distribution scheme. Their scheme enforces each node to randomly select a subset of keys from a pool of keys under a certain probability that any two nodes share at least one common key. Chan, Perrig, and Song [21] improved the security of previous scheme by proposing a q-composite random key pre-distribution scheme. Their scheme allows two sensor nodes to create a pairwise key in between if they share at least q-common pre-distribution keys ($q \geq 1$) in their subsets.

Donggang Liu, and Peng Ning [22] proposed a polynomial pool-based key pre-distribution framework which can be considered a combination of both ideas of [20], [21]. Their framework has three phases: a **setup phase** where a setup server uses nodes' IDs for randomly generates a pool of multiple bivariate t-degree polynomials and assigns a subset of these polynomial shares to each sensor node. The second phase, **Direct Key Establishment phase**, establishes a direct secure channel between two nodes only if they share on the same bivariate polynomial in their subsets. In the final **Path Key Establishment phase**, if there are no common polynomial shares between two sensor nodes, both nodes try to connect with an intermediated node(s) adjacent to them as in phase 2. These intermediated nodes act as a communication path (route) between previous two nodes.

IV. THE EXPERIMENTS AND SIMULATION RESULTS

As described previously, the A3 as a topology control protocol has specific characteristics that constraint the construction of a Parent-Child relationship according to selection metrics of remaining energy and distance between nodes. The use of a key pre-distribution technique as the polynomial pool-based key pre-distribution framework proposed in [22] can negatively impact the performance of the A3 algorithm. The experiments evaluate different scenarios of applying the polynomial pool-based key pre-distribution framework under different probability of two neighbors sharing on a common polynomial.

The experiments run on Atarraya simulator [10], [13], [23] with predefined parameters described in Table I.

The simulation experiments show that applying a key pre-distribution scheme using small probabilities *(p)* will increase the number of active nodes and will throw away the properties of the A3 protocol especially in small-sized networks as it is plotted in Table II. Increasing numbers of active nodes will significantly increase the energy consumption rate as it illustrated in Figure 3. The previous results reduce the performance of the network running the A3 algorithm and in future this will affect on the lifetime of that network.

For the purpose of testing the effects of key pre-distribution scheme on the lifetime of the network, the paper uses the DGTTRec topology maintenance algorithm in conjunction with the A3. As it was proved that the increasing amount of active nodes will consumed more of the network's energy. This extra consumption of energy will decrease the

Table I
SIMULATION PARAMETERS.

Parameter	Value
Deployment Area	600 x 600
Number of Nodes	200,400,600,800, and 1000
Number of Sinks	1 sink node
Node Location Distribution	Uniform (600,600)
Max Transmission Range	38m
Sensing Range	119m
Inter-Execution Timer(for DGTTRec)	7200 seconds (2 hours)
Time Threshold	1000 time units
Initial Energy	3200 mA-h
Node Energy Distribution	Uniform
Processor	Active=8mA — Sleep=15μA
Sensor	Active=5mA — Sleep=5μA
Radio	Tx_Consumption=12mA — Rx_Consumption=7mA — Sleep=1μA
Message length	Short: 40 bytes — Long: 100 bytes

Table II
NUMBER OF ACTIVE NODES BASED ON DIFFERENT PROBABILITY p.

Number Of Nodes	p= 0.35	p=0.55	p= 0.75	Original A3
200	74	52	50	36
400	92	65	53	33
600	97	75	66	40
800	88	73	66	45
1000	99	76	67	40

network's lifetime. Figure 4 showed that the topology with the highest probability had a better network's lifetime than other probabilities.

To conclude, the simulation results showed that a gradual increase in the probability implemented by the key pre-distribution scheme leads to gradual improvement in the performance of the A3 protocol. This improvement encompasses a reduction in the number of active nodes, a reduction in the total network's spent energy, and an increase in the whole network's lifetime. This paper offers an important recommendation pertinent to this finding; high probability used in the key pre-distribution scheme proposed in [22] for securing a topology control is preferable ($p \geq 0.75$). The higher the probability, the higher the number of keys saved in each node's memory space. Although the number of keys will increase, this leads to an optimally secured and reduced topology; hence, increases the network's lifetime.

V. CONCLUSIONS

This paper was an attempt to identify whether it is practical to apply a key pre-distribution scheme on topology control protocols, and determine the constraints to be considered in this application. As seen from the simulation results, the implementation of a key pre-distribution scheme based on a probability of any two nodes sharing at least one common key, may negatively impact the performance of topology control protocols. Nevertheless, the application of high-probability key pre-distribution schemes - with a value higher than 0.75 - has positive effects. In order to approach optimal secured topology control performance, this probability value should approximate 0.99. The main aim of this investigation was to open a new research point worth of further research in regards to the construction of a new key pre-distribution security scheme to be applied in topology control protocols.

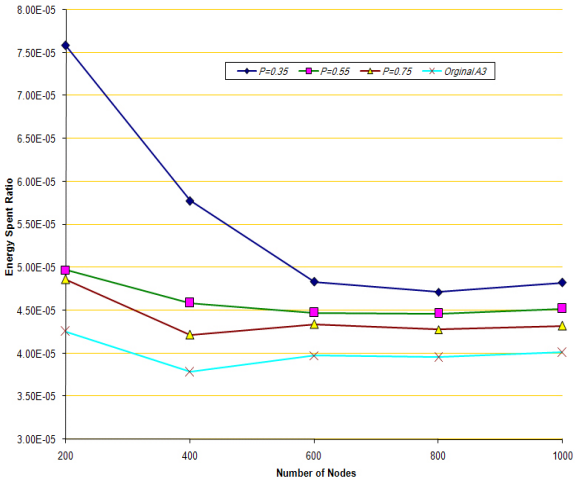


Figure 3: The energy spent ratio using different probabilities p.

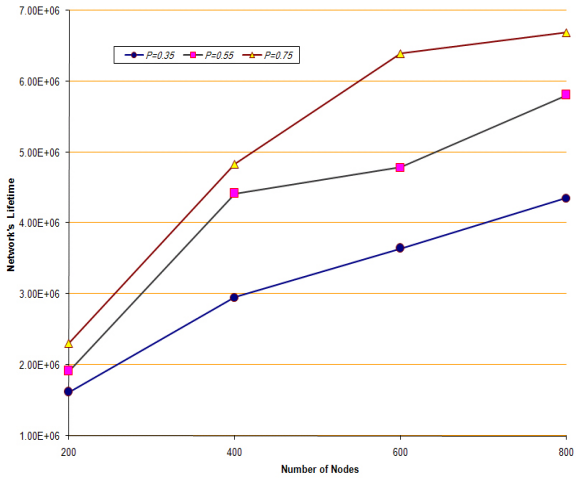


Figure 4: The lifetime of the WSN.

REFERENCES

[1] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, "Security Issues in Wireless Sensor Networks", International Journal of Communications, Issue 1, Vol. 2, 2008

[2] Neal Koblitz, Alfred J. Menezes, "A survey of public-key cryptosystems", SIAM Review, Vol. 46, 2004, pp. 599-634.

[3] Haowen Chan, Adrian Perrig, Dawn Song. "Random Key Predistribution Schemes for Sensor Networks", In Proceedings of the IEEE Symposium on Security and Privacy, 2003.

[4] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor network survey", Computer Networks Elsevier 52, 2008, pp. 2292-2330.

[5] Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks", ACM Conference on Computer and Communications Security, 2003, pp. 42-51.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, vol. 22, November 1976, pp. 644-654.

[7] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, no. 2, 1978, pp. 120-126.

[8] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "Spins: Security protocols for sensor networks", in Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Rome, Italy, July 2001, pp. 189-199.

[9] Donggang Liu, Peng Ning, Rongfang Li, "Establishing pairwise keys in distributed sensor networks", ACM Trans. Inf. Syst. Secur., Vol. 8, No. 1, February 2005, pp. 41-77.

[10] Wightman, P.M. Labrador, M.A., "A3: a topology control algorithm for wireless sensor networks", In Proceedings of the IEEE GLOBECOM, 2008.

[11] P. Santi, "Topology control in wireless ad hoc and sensor networks", ACM Computing Surveys, vol. 37, no. 2, 2005, pp. 164-194.

[12] Bao, L., Garcia-Luna-Aceves, J., "Topology management in ad hoc networks", In Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2003, pp. 129-140.

[13] Miguel A. Labrador, Pedro M. Wightman, "Topology Control in Wireless Sensor Networks - with a companion simulation tool for teaching and research", Springer, 2009.

[14] M. Kubisch, H. Karl, A. Wolisz, L. C. Zhong, and J. Rabaey, "Distributed algorithms for transmission power control in wireless sensor networks", in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '03), New York, NY, USA, March 2003, pp. 558-563.

[15] N. Li, J. C. Hou, and L. Sha, "Design and analysis of an MST-based topology control algorithm", in Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies (IEEE INFOCOM '03), vol. 3, San Francisco, Calif, USA, March-April 2003, pp. 1702-1712.

[16] Pedro Wightman, Miguel A. Labrador, "Topology Maintenance: Extending the Lifetime of Wireless Sensor Networks", In Proceedings of Latincom, 2009.

[17] Prim, R., "Shortest connection networks and some generalizations", Bell Syst. Tech. J. 36, 1957, pp. 1389-1401.

[18] S. Guha and S. Khuller, "Approximation algorithms for connected dominating sets", Proc. of 4th Annual. European Symposium on Algorithms, Springer, pp. 179-193.

[19] Pedro Wightman, Miguel A. Labrador, "Reducing the communication range or turning nodes off? An initial study for wireless sensor networks", A Research Article, Ingenieria and Desarrollo, Universidad del Norte, Numro 28, 2011.

[20] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", in Proceedings of the 9th ACM conference on Computer and communications security, Washington DC, USA, November 2002, pp. 41-47.

[21] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks", in IEEE Symposium on Security and Privacy, Berkeley, California, May 2003, pp. 197-213.

[22] Donggang Liu, Peng Ning. "Security for Wireless Sensor Networks". Advances in Information Security, Vol. 28. Springer. December 2006, pp. 63-76.

[23] Pedro Wightman, "Atarraya: A topology control simulator". http://www.cse.usf.edu/ labrador/Atarraya/.