International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 3 – MARCH 2018.

ENHANCED MESSAGE AUTHENTICATION USING HOP-BY-HOP ROUTING ALGORITHM

RAJAPRIYA.J[#1] and KALAISELVI.G[*2]

[#] *M.Phil. Scholar, Dept. of Computer Science, Krishnasamy College of Science, Arts & Management for Women, Cuddalore, India*

[*] *Asst. Prof. & HOD, Dept. of Computer Science, Krishnasamy College of Science, Arts & Management for Women, Cuddalore.*

***Abstract*— Message authentication plays a vital part in thwarting unauthorized and tainted messages from being sent in mobile nodes to spare the valuable energy. Therefore, numerous authentication plans have been proposed in literature to give message authenticity and trustworthiness check for mobile computing systems. But, the greater part of them has the restrictions of high computational and communication overhead, in addition to absence of scalability and strength to node compromise attacks. This study introduced a message authentication model under key pre-distribution scheme using hop-by-hop algorithm. Since, routing path is an essential activity in the field of computing systems. We have used Single path routing and any path routing process which specifically employed to pick the optimal route from set of different routes. The role of single path routing algorithm is to optimize the path between the sender and receiver node. Similarly, the role of any path routing algorithm is to select the best path between the sender and receiver node. Both the routing process failed to solve the issue of security in the network layer path. Authentication is one of the security parameters that need to be upgraded in the message processing systems. Current security processes are lined up by symmetric key cryptosystems or public key cryptosystems. The objective of the proposed model is to reduce the computational cost and communication overhead. A verification model is introduced between sender and receiver node which contain infinite number of messages. Experimental results have shown the efficiency of the proposed message authentication model in terms of cost minimization model.**

***Index Terms*— Message authentication, Mobile computing, Attackers, Hop-by-hop algorithm, Network layer, Cost minimization and communication overhead.**

I. INTRODUCTION

Key management is an important part of the network security systems. To securely access the devices or data, key should be effectively managed and prioritized. Key Management is defined as "the set of techniques and procedures supporting key establishment and the maintenance of keying relationships between authorized parties". Key management is the set of cryptographic method that ensure the security parameters like data confidentiality, integrity, authentication, and digital signatures [1].

Message authentication is an important concept in the field of network security. Message Authentication is defined as the secure transfer of message between intended sender and intended receiver. This data transmission process involves the key management systems. Confidentiality and security to the data is actually provided by an authentication. Authentication involves the confident identification of one party by another party or a process of confirming an identity. But nowadays there are various methods for authentication such as Message Authentication Code, Signcryption, and Key Aggregate System are emerged very rapidly for better security precaution [2].

The benefits of the key management systems in message authentication process are presented as follows:

Scalability: the total number N of nodes accommodated by the key management technique. In KPSs this parameter is typically limited by the memory available on WAHN nodes to store keying material.

Resource Performance: computational and communication efficiency level and storage requirements on nodes.

Feasibility for mobile ad hoc networking: ability to enable performance-aware (scalable as well as energy and time efficient) key establishment (and, thus, security) in dynamic WAHNs, where WAHN membership and size is a priori unknown.

Connectivity properties: measures the probability that two nodes can establish a pairwise key. A key management technique with perfect connectivity enables direct pairwise key establishment [3].

In this paper, we have proposed a novel message authentication scheme using key management systems. In order to securely transfer the message via public channel, the authentication should be incorporated. A key pool for key pre-distribution schemes that is built based on symmetric cryptography concepts contains secret pairwise keys. The size of the key pool in addition to the key ring size directly affects cryptographic connectivity of a network. In order to be able to establish a secure communication path, a source node has to find a network layer path to a destination node first [4]. Then, two adjacent nodes forming a network layer hop check whether or not they have at least one key in common. If so, they can communicate securely. Otherwise, they have to find a cryptographic path amongst themselves [5].

The rest of the paper is organized as follows:

Section II describes the related work; Section III presents the proposed work; Section IV presents the experimental analysis and concludes in section V.

II. RELATED WORK

This section reveals the prior works on the message authentication schemes of the routing systems. In, symmetric key and hash based authentication schemes were proposed for WSNs. In these schemes, each symmetric authentication key is shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node [5]. Therefore, these schemes are not resilient to node compromise attacks. Another type of symmetric-key scheme requires synchronization among nodes. These schemes, including TESLA and its variants, can also provide message sender authentication. However, this scheme requires initial time synchronization, which is not easy to be implemented in large scale WSNs. In addition, they also introduce delay in message authentication, and the delay increases as the network scales up. A secret polynomial based message authentication scheme was introduced in. This scheme offers information- theoretic security with ideas similar to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. When the number of messages transmitted is below the threshold, the scheme enables the intermediate node to verify the authenticity of the message through polynomial evaluation. However, when the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken [6]. To increase the threshold and the complexity for the intruder to reconstruct the secret polynomial, a random noise, also called a perturbation factor, was added to the polynomial in to thwart the adversary from computing the coefficient of the polynomial.

However, the added perturbation factor can be completely removed using error-correcting code techniques. For the public-key based approach, each message is transmitted along with the digital signature of the message generated using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key [7]. The recent progress on ECC shows that the public-key schemes can be more advantageous in terms of memory usage, message complexity, and security resilience, since public-key based approaches have a simple and clean key management. The existing anonymous communication protocols are largely stemmed from either mixnet or DC-net. A mixnet provides anonymity via packet re-shuffling through a set of mix servers (with at least one being trusted). In a mixnet, a sender encrypts an outgoing message, and the ID of the recipient, using the public key of the mix.

A secret polynomial based message authentication scheme was introduced in [8]. This scheme offers information-theoretic security with ideas similar to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. When the number of messages transmitted is below the threshold, the scheme enables the intermediate node to verify the authenticity of the message through polynomial evaluation. However, when the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken. To increase the threshold and the complexity for the intruder to reconstruct the secret polynomial, a random noise, also called a perturbation factor, was added to the polynomial in [9] to thwart the adversary from computing the coefficient of the polynomial. However, the added perturbation factor can be completely removed using error-correcting code techniques [10]. For the public-key based approach, each message is transmitted along with the digital signature of the message generated using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key. The recent progress on ECC shows that the public-key schemes can be more advantageous in terms of memory usage, message complexity, and security resilience, since public-key based approaches have a simple and clean key management [11].

In public-key based technique [12] each message contains digital signature of message which is created by using private key of sender. Each of mediatory nodes as well as destination node can authenticate the message using public-key of sender. A drawback of this method is large computational overhead. Recently, process on elliptic curve cryptography [13] resulted that public-key methods are more beneficial in case of computational difficulty, utilization of memory and flexible security. It is possible when management of public-key is easier and elegant. Author [14] introduced a Statistical Encourse Filtering (SEF) methodology to find and eliminate the corrupt messages. SEF have need of every message is authenticated on the basis of message authentication codes (MACs) as well as each created by a node identifies the similar event. A message is authenticated by each node as well as observed the accuracy and drops corrupt messages by MACs [15]. Further, sink node eliminates paths which contains corrupt message. SEF utilizes all performance of system to find out the integrity of every message by total selection creating by various recognizing nodes and collect false-message-location by various sending nodes. Author's examination shows with an overhead for every message SEF is capable to eliminate injected corrupt messages by exchange node within sending bounces and decrease energy utilization.

III. PROPOSED WORK

This section describes the proposed method of our study. In this work, we have proposed message authentication model under key pre-distribution management over the overlay routing process. Though, variety of routing paths has been explored to find the optimum one in order to transmit the messages in the network layer. We have framed linear distance optimization model that make use of Single path routing and any path routing systems. Prior works suggested two sorts of routing protocols, namely Single path routing and any path routing systems. The role of single path routing algorithm is to optimize the path between the sender and receiver node. Similarly, the role of any path routing algorithm is to select the best path between the sender and

receiver node. Both the routing process failed to solve the issue of security in the network layer path. Authentication is one of the security parameters that need to be upgraded in the message processing systems. Current security processes are lined up by symmetric key cryptosystems or public key cryptosystems. The objective of the proposed model is to reduce the computational cost and communication overhead. A verification model is introduced between sender and receiver node which contain infinite number of messages. The project aims to develop in Java that provides message authentication model between sender and intended receiver under key pre-distribution schemes. Privacy is the major concern that has to devise from any public channel. Henceforth, hop-by-hop routing process is initiated in the network k layer. The working principle of this research study is presented as follows:

A. Routing path:

This module depicts the prediction of the routing path between the sender and receiver. The receiver node r should properly select from the set of receivers without compromising the security and performance of the systems. The scheme should be modeled from the encryption and decryption steps. Linear distance optimization model is used as the objectives function between overlay and underlay distance. In order to evaluate the performance and security strength of the proposed algorithm, we apply it to a number of asymmetric and symmetric key pre-distribution schemes.

B. Key Pre-Distribution process:

Key pre-distribution process is a significant process in our proposed model. On-demand routing protocols have been initiated for symmetric and asymmetric key models. A weighted directed graph is modeled between sender and receiver nodes. Here, G (V, E) is a static graph where all nodes can be pre-loaded with the lookup table at the initialization of the network. The pre-loaded table does not contain the cost of edges at this stage. At the network operation phase, each node finds the underlay path length associated with its overlay neighbors by sending simple route requests.

C. Cost minimization model:

This model is used for users for minimizing the cost of file transferring process from sender to recover. Path cost minimizing collection reflects the best possible performance of the path. SASR algorithm calculates the spatial reusability aware path cost of it. Then, the path with the smallest cost can be selected. In a spatial reusability-aware path cost evaluation for single-path routing a given each of the paths found by an existing source routing protocol (e.g., DSR), our SASR algorithm calculates the spatial reusability aware path cost of it. Then, the path with the smallest cost can be selected.

D. Formation of shortest paths

The shortest path is formed from the single path routing and any path routing process. A pairwise key is generated from the Message Authentication model. We have used spatial reusability aware single-path routing and any path routing process. SASR-MIN tends to exploit the best performance of the paths; the other category (SASR-MAX) evaluates the performance of the paths in the worst case. Given each of the paths found by an existing source routing protocol (e.g., DSR, our SASR algorithm calculates the spatial reusability aware path cost of it. Then, the path with the smallest cost can be selected. Here, we use approximation algorithm for finding the path delivery time minimizing collection of non-interfering sets, namely SASR-MIN algorithm, when the collection of all the maximal non interfering sets on path P can be calculated efficiently.

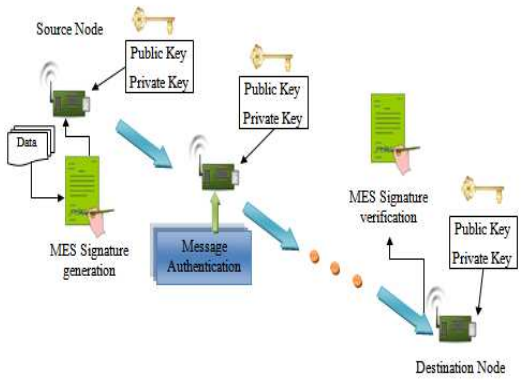


Fig.1 Proposed architecture

IV. EXPERIMENTAL RESULTS

This section depicts the experimental analysis of our proposed work.

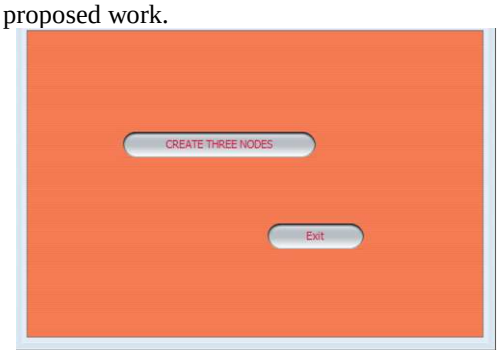
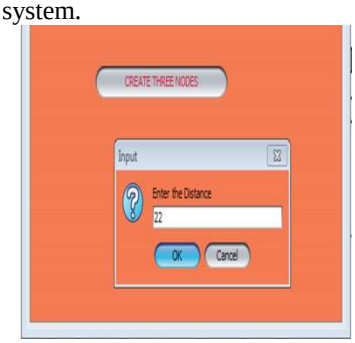


Fig. 2. Creation of three nodes

The above fig.2 represents the wireless node creation. It indicates the setup process of our proposed method. We initialized set of static nodes before doing the message authentication system via pre-distributed key management system.



a) Node's creation using distance *b) Node's creation using range*

Fig. 3 (a) & (b). Node's creation using range and distance model

The above fig. 3 depicts the creation of static nodes using range and distance metrics. In this process, we define the range i.e communication range between sender and destination node and distance i.e how long the nodes are to be placed.

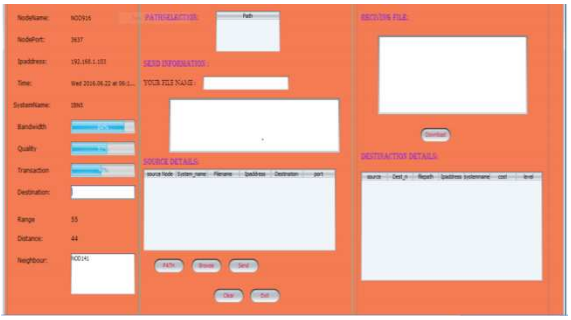


Fig.4. Finding the nearest neighboring nodes for path creation

The above fig.4 represents the discovery of nearest neighboring nodes. Efficient path creation is the main attribute of our proposed scheme. The intent is to find the nearest nodes between sender and destination node in order to create efficient routing path based on the range and distance metric.

Fig.5. Selecting the destination node from its neighboring node's information

The above fig.5 represents the selection of destination node. In this step, an appropriate destination node is selected using the neighboring node's information. The intent of this step is to discover the accurate destination node to eradicate the misuse of packets.

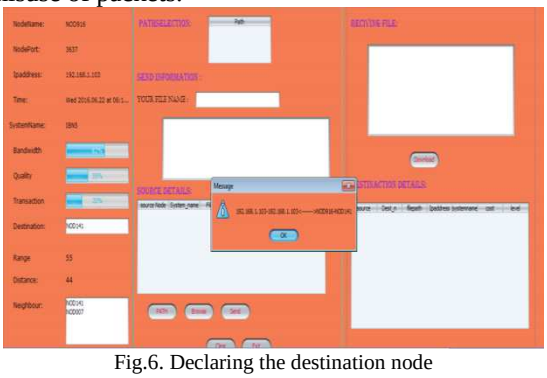


Fig.6. Declaring the destination node

The above fig. 6 represents the finalization of the destination node from the set of destination node. Relied upon the neighboring node's information, the destination node is selected.

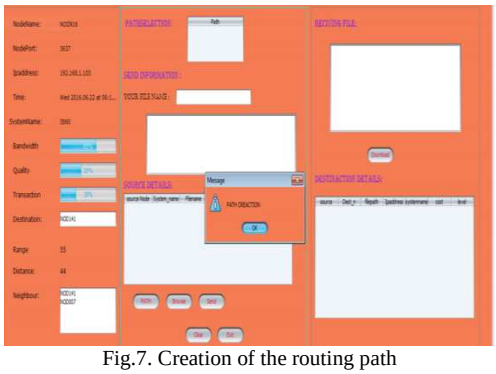


Fig.7. Creation of the routing path

The above fig.7 presents the routing path. Once the destination node is finalized, the routing path is formed. Depending on the distance value, the source node, intermediate node and destination node are declared.

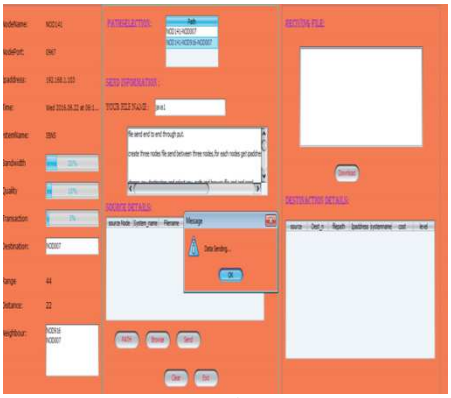


Fig. 8. Once path is created, the data is forwarded to the intended destination

The above fig. 8 depicts the data transmission process. Once the routes are declared, the packets are transmitted from source node to the intended destination node.

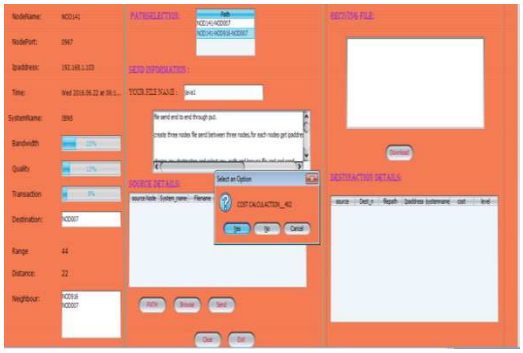


Fig.9. Cost of the selected path is estimated

The above fig. 9 indicates the cost analysis of the selected path. Since, cost analysis is one of our proposed metric. In this step, we have analyzed the cost value for the selected routing path. It is purely based on the size and length of the message packets and no.of intermediate nodes used for the data transmission process over wireless environment.

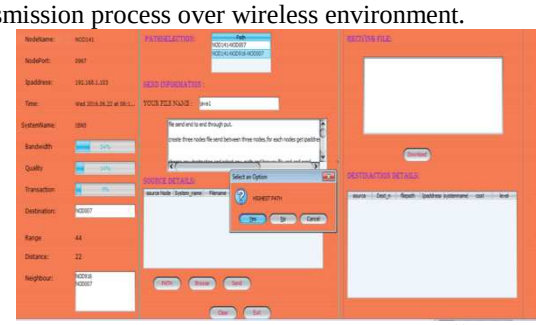


Fig.10.Selecting the optimal path i.e cost-wise efficient

The above fig.10 depicts the selection of optimal path. The cost analysis is done for the set of possible routes in the

wireless environment. For each routing path, the cost factor is estimated. Depending upon the estimated cost, the efficient route is selected. Here, we have declared lower the cost value will depicts the efficient routing process. Henceforth, the efficient routing system implicates the lower cost factor.

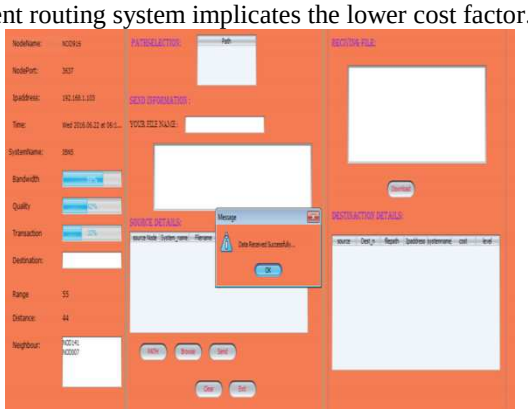


Fig.11. Successful transmission of message to its intended receiver

The above fig.11 presents the transmission of message to its correct destination node. Once the routes are finalized, the message is initiated by the sender node to the routing path. Along with the message, the destination address is mentioned and finally, the message is received by the destination node.

Fig.12 Creation of the multipath for securely transmitting message

The above fig.12 depicts the creation of multipath for message transmission process. Initially, we have analyzed for the single path routing protocols which consumes higher time. To resolve this issue, in addition, we have also analyzed multipath routing system. The objective of the study is to securely transmit the message using efficient routing system. In this step, we have collectively analyzed the possible routes for generating multiple paths to avoid the misuse of routes as well as message from the adversary's.

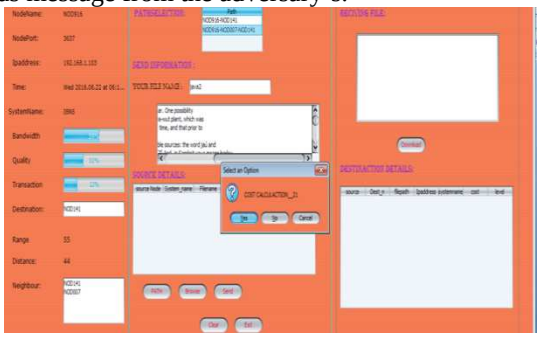


Fig.13. Similarly, the calculation of the cost for all nodes in the networks

The above fig.13 depicts the cost calculation for the possible multiple paths. Between the sender and destination node, the intermediate nodes are the backbone for achieving efficient routing systems. Similarly, we have analyzed the cost for each possible route to eliminate the time consumption and for speedier message transmission.

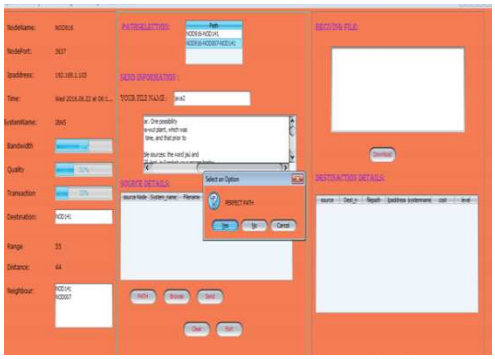


Fig. 14. Selecting the optimal path from set of different paths.

The above fig.14 depicts the optimal path from set of multiple paths. Once the cost is analyzed for possible routes, efficient routes are picked for further process.

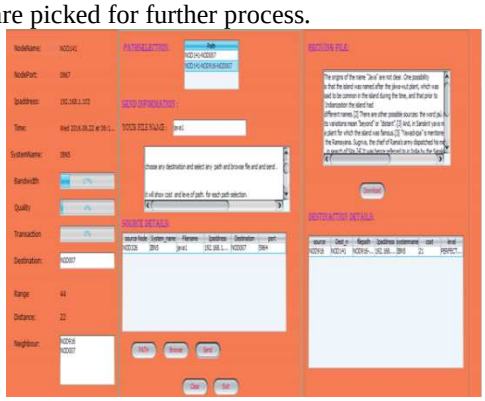


Fig.15. Destination viewing the file

The above fig.15 depicts the destination node viewing the received message. Once the message is securely received by the destination node, acknowledgments send back to the source node. It proves that the message authentication process is successfully achieved.

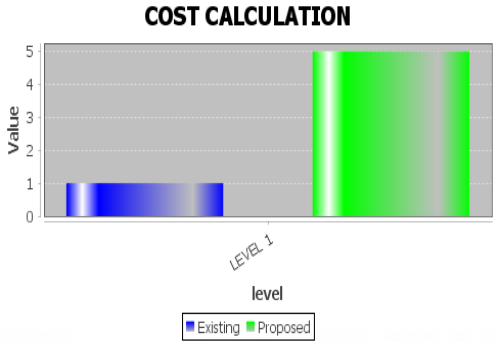


Fig.16. Different levels of cost calculation between existing and proposed system

The above fig. 16 depicts the cost comparison between existing and proposed system. The cost value for each route is calculated. Based on the estimated cost values, the optimal route is determined.

V. CONCLUSION

Due to the limited availability of the energy, it is extremely important to carefully select the optimal route which can increase the end-to-end throughput, especially in hop-by-hop routing process. Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded between mobile nodes. In this work, we have enhanced message authentication model under key pre-distribution scheme using hop-by-hop algorithm. Since, routing path is an essential activity in the field of computing systems. We have used Single path routing and any path routing process which specifically employed to

pick the optimal route from set of different routes. The role of single path routing algorithm is to optimize the path between the sender and receiver node. Similarly, the role of any path routing algorithm is to select the best path between the sender and receiver node. Both the routing process failed to solve the issue of security in the network layer path. Authentication is one of the security parameters that need to be upgraded in the message processing systems. Current security processes are lined up by symmetric key cryptosystems or public key cryptosystems. The objective of the proposed model is to reduce the computational cost and communication overhead. A verification model is introduced between sender and receiver node which contain infinite number of messages. Experimental results have shown the efficiency of the proposed message authentication model in terms of cost minimization model.

REFERENCES

[1] Mohammed Gharib et al, "Secure Overlay Routing Using Key Pre-Distribution: A Linear Distance Optimization Approach", IEEE transactions on Mobile Computing, 20 (6), 2016.

[2] S. Ruj, A. Nayak, and I. Stojmenovic, "Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs," in INFOCOM, 2011 Proceedings IEEE, April 2011, pp. 326–330.

[3] W. Bechkit, Y. Challal, A. Bouabdallah, and V. Tarokh, "A highly scalable key pre-distribution scheme for wireless sensor networks," Wireless Communications, IEEE Transactions on, vol. 12, no. 2, pp. 948–959, February 2013.

[4] M. e. a. Gharib, "A novel probabilistic key management algorithm for large-scale manets," in Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on, March 2013, pp. 349–356.

[5] 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, ser. CCS '02. New York, NY, USA: ACM, 2002, pp. 41–47. [Online]. Available: http://doi.acm.org/10.1145/586110.586117

[6] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Security and Privacy, 2003. Proceedings. 2003 Symposium on, May 2003, pp. 197–213.

[7] M. e. a. Gharib, "Expert key selection impact on the manets' performance using probabilistic key management algorithm," in Proceedings of the 6th International Conference on Security of Information and Networks, ser. SIN '13. New York, NY, USA: ACM, 2013, pp. 347–351.

[8] T. Choi, H. B. Acharya, and M. Gouda, "The best keying protocol for sensor networks," in Proceedings of IEEE WoWMoM, June 2011.

[9] S. Zhu, S. Setia, and S. Jajodia, "Leap: Efficient security mechanisms for large-scale distributed sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security, ser. CCS '03. New York, NY, USA: ACM, 2003, pp. 62–72.

[10] S. Ruj and B. Roy, "Key predistribution using combinatorial designs for grid-group deployment scheme in wireless sensor networks," ACM Trans. Sen. Netw., vol. 6, no. 1, pp. 4:1–4:28, Jan. 2010.

[11] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security, ser. CCS '03. New York, NY, USA: ACM, 2003, pp. 52–61.

[12] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in Information Processing in Sensor Networks, 2008. IPSN '08. International Conference on, April 2008, pp. 245–256.

[13] Z. Liu, J. Ma, Q. Huang, and S. Moon, "Asymmetric key pre-distribution scheme for sensor networks," Wireless Communications, IEEE Transactions on, vol. 8, no. 3, pp. 1366–1372, March 2009.

[14] E. F. Assmus and J. D. Key, Designs and their codes. Cambridge University Press, 1992.

[15] M. Huson and A. Sen, "Broadcast scheduling algorithms for radio networks," in Military Communications Conference, 1995. MILCOM '95, Conference Record, IEEE, vol. 2, Nov 1995, pp. 647–651 vol.2.