Random Key Pre-Distribution Techniques against Sybil Attacks

Mohammad Ehdaie[*], Nikos Alexiou[+] and Panos Papadimitratos[+]
[*]*Parsa Sharif Research Center, Tehran,* [+]*KTH, Stockholm, Sweden*
ehdaie@parsasharif.ir, alexiou@kth.se, papadim@kth.se
Corresponding author: Mohammad Ehdaie

***Abstract*- Sybil attacks pose a serious threat for Wireless Sensor Networks (WSN) security. They can create problems in routing, voting schemes, decision making, distributed storage and sensor re-programming. In a Sybil attack, the attacker masquerades as multiple sensor identities that are actually controlled by one or a few existing attacker nodes. Sybil identities are fabricated out of stolen keys, obtained by captured benign nodes. Existing Sybil defensive mechanisms suffer from the restricted sensor network size, or cause excessive resource consumption for the sensor network. In this work we propose a Sybil node detection mechanism, based on Random Key Distribution (RKD) schemes that can cope with large network sizes and minimize the waste of resources. We explain the techniques each node can use in a network running q-composite RKD to detect Sybil identities and restrict their number. Our method requires no trust to other sensors, which is important to defend against the attack.**

***Index Terms*-** Random Key Predistribution, Sybil Attack, Wireless Sensor Networks.

I. INTRODUCTION

Wireless Sensor Networks (WSN) consist of just a few, some hundreds or even thousands of wireless sensors, depending on the particular application of the sensors. Applications can range from on-body sensors, where confidentiality, privacy and authenticity are the main security requirements, to tactical networks that have additional considerations, such as secure routing or network re-programming. Wireless sensors are small devices with limited computing and storage capabilities, and thus scarce sensor resources are a main consideration for WSN security.

In order to secure the network, we need to distribute keys between the nodes. Key Distribution Schemes (KDS) define the way that sensors establish a shared secret key to communicate securely. In a Random Key Distribution (RKD) scheme, each node is assigned a set of keys, randomly chosen from a large key space, called the key pool. Two neighboring nodes, follow a Key Discovery Protocol (KDP) in order to find overlaps in their key rings, which are the set of keys stored at each sensor. If

Manuscript received 8-Nov.-2015 and revised 16-March-2016,
Accepted on 5- May-2016
P- ISSN: 2322-4088
E- ISSN: 2322-3936

common keys are found during the key discovery process, the sensors can establish a secure communication channel, with a new key derived from the shared ones.

RKD schemes usually do not consider strict authentication mechanisms. Authentication in sensor networks has some costs. It limits supported network size and make network deployments difficult; especially in case of node addition and node removal. Using a trusted identification authority, such as in a Public Key Infrastructure (PKI), is the only means to achieve authentication in a sensor network. However, implementing a PKI for WSNs has major problems. Public key cryptography requires costly computations, which waste the limited sensor resources and thus, gives the potential to launch Denial of Service attacks. In other words, since PKI is power-consuming and waste nodes' resources, an adversary can make nodes to run PKI operations multiple times and then discharge nodes. Therefore, attacked nodes will be out of access (DoS attack). A trusted identification authority is the only way to achieve total resilience against the Sybil attack [1]. Lack of authentication in WSNs is a vulnerable point for security against the attack.

In a Sybil attack, the adversary masquerades as multiple sensor identities and presents them to the network. Multiple instances of a stolen key ring can be presented to a victim sensor, which cannot distinguish between a legitimate and a Sybil identity. Sybil attacks can cause a plethora of security issues, including but not limited to secure routing, node revocation and voting schemes, decision making, distributed storage and redundancy schemes [1]. Moreover, reprogramming of sensor networks, implemented using code segmentation mechanisms and code redundancy schemes [2], is susceptible to the attack.

Existing Sybil attack countermeasures, like resource testing, suffer from the problem of extreme resource consumption. However, in the case of resource testing, a restricted set of nodes that have been verified can have a great benefit for the network, by reducing the cost of the verification. It is therefore important to have flexible defensive mechanisms against Sybil attacks that can support larger network sizes, and also achieve a minimal consumption of resources.

In this study we propose a decentralized Sybil detection approach, based on random key pre-distribution schemes. While there are some papers [14], [15], [18], [23] that propose a RKD to improve resistance against Sybil attack, no one uses a current known RKD like q-composite to detect Sybil attack, according to our best knowledge. We introduce a new method to stand with Sybil in a network running q-Composite RKD. Our scheme relies only on the knowledge that each sensor has of its own key ring and which keys are used to communicate with the neighboring nodes. We do not consider any trust relations between the sensors, which is important to defend against the attack. We achieve a massive reduction in terms of cost needed to identify the Sybil identities, compared to other approaches. We limit the number of Sybil identities that can be successfully introduced by the adversary, and show that this number is sustainable by a plethora of applications, otherwise vulnerable to the attack. Our scheme is flexible and can support large network sizes. It can also be

used to improve the effectiveness of other Sybil defensive techniques, such as resource testing. We test our approach for different adversarial strategies and prove that it is effective. To the best of our knowledge there are no other works that consider a node-centric Sybil detection strategy, similar to our scheme.

The remainder of this paper is organized as follows: The problem statement and assumptions are given in Section 2. Section 3 deals with the main work, i.e. introducing different strategies that an adversary may follow to mount a Sybil attack, as well as proposing the defenses against them. In Section 4 we review the current countermeasures against Sybil attack. Finally, Section 5 concludes the paper and notes the ideas of our future work.

II. PROBLEM STATEMENT & SYSTEM MODEL

Several works have proposed Random Key Pre-Distribution Techniques for WSN, as the way to establish secure communication channels between wireless sensors [3]-[6]. Each node is equipped with a key ring of size m, chosen randomly from a large Pool of keys of size P. Using its key ring, each sensor can discover common keys with other neighboring nodes, following a KDP. In this part we briefly discuss the main RKD schemes that exist in the literature.

In the basic random key pre-distribution scheme, two nodes aim at discovering one common key out of the m stored in their key rings. The shared key can then be used to establish a secure channel between the sensors. In the q-composite scheme, two sensors have to follow the KDP and discover at least q common keys, in order to establish a secure connection. The common key is computed out of the shared ones. Random pairwise key distribution techniques associate each node identity with a key, included in a sensor's key ring. Different proposals include the single-space pairwise key distribution technique, as well as the multispace scheme extension [7]. In multi-space approaches each sensor is assigned some key spaces. To establish a secure connection, two sensors have to discover a common key space and then their shared secret.

We consider an adversary that launches a Sybil attack against a WSN that runs a q-composite RKD scheme[1]. The adversary is powerful enough to capture nodes and steal their key rings. The aim of the adversary is to introduce as many Sybil identities as possible to the network. We assume that the adversary cannot register any node in the network (and get a key ring directly from P). We also consider any number of devices can be planted in the network sharing the stolen key ring, since this would not affect the effectiveness of our scheme. It is also assumed that an adversary knows nothing about key sets of other nodes without help of KDP. We also note that following the KDP, two parties can only discover the common keys they share, the importance of which is discussed for an attack

[1] *The basic scheme and the q-composite scheme are extensively used in sensor network applications. We can also consider the basic RKD scheme with a few modifications.*

involving colluding adversaries, in [8]. For this version of the paper we consider the case where only one key ring is captured. The extension of our scheme for multiple captured key rings and colluding adversaries is included in our future work.

In the remainder of the paper, we use the following notations:

- A or A_i: The adversarial nodes; the nodes that are captured by the adversary
- B or B_i: Benign nodes
- K_X: Key ring of node X
- m: Size of key ring
- P: Size of key pool
- q: minimum required number of common keys for two nodes to start communication
- p_c: Probability that each pair of nodes has at least q common keys
- SP: Sensor Profile generated by the set of common keys discovered during the KDP. Defined in section 3.
- x: The number of keys shared between the two nodes considered for the analysis, especially the victim and the adversary.

III. OUR APPROACH

Lack of authentication in sensor networks gives a back-door vulnerability for Sybil attacks. Implementing strict authentication schemes, such as in the pairwise scheme, unavoidably has a great impact to the size of the supported network, and can create additional problems as discussed in section 4. Moreover it can create connectivity problems for sparse networks, or even sensor networks with mobility.

Following the KDP, each sensor discovers the common keys it shares with its neighbors. Each sensor, based on this set of shared keys, can create a Sensor Profile (SP) for each of its neighbors. Profiles are the set of common keys SP = $\{K_1, \ldots, K_x\}$, where K_i is the i-th common key. We formalize the definition of a SP as follows:

Definition 1. A sensor profile SP, is an identifier assigned from a node to a neighbor, and is the set of the shared keys discovered during the KDP.

We show that SPs, are distinct with high probability, and can serve as authentication means for neighboring sensors. This means that each SP will probably be distinct for a sensor's neighbors with high probability, under normal conditions. Each sensor can create SPs of its own neighbors that can be used to identify the Sybil nodes. We prove that they can be used to detect most of the Sybil nodes, and greatly restrict the attacker's capabilities of generating large numbers of Sybil identities. Considering the motive of the attack, which is to introduce as many Sybil nodes as possible, the result

is serious. Following a relaxed authentication approach using SPs in the q-composite scheme, we keep the benefits of the scheme, while securing the network against large scale Sybil attacks. The scheme also works on a per-sensor level, which is crucial to defend against the attack, since it does not require sensor cooperation or trust schemes that could be compromised by the attack.

We observe that the Sybil SPs have many overlaps. The reason is that the adversary fabricates the Sybil identities from one (or a limited number of) captured key ring(s), which is much smaller than the size of the key pool P. This observation deviates from the general case presented above that the SPs are distinct with a very high probability. Therefore, similar SPs can be the result of a Sybil attack, and can form a set of suspected Sybil nodes for each sensor. This set of suspect nodes can then serve as an input to resource testing techniques, or be discarded from the list of neighbors.

We now discuss the effectiveness of our scheme by studying four strategies that an adversary can follow to fabricate Sybil identities.

A. Strategy 1: The naive attacker strategy

In the first case, a naive adversary presents herself to a benign node, say B, and then fabricates a new Sybil identity, by presenting exactly the same key ring to the victim node. The adversary first runs the KDP between B and A_1, the first Sybil node, and their shared keys are revealed to both of them. Using these keys, the adversary fabricates A_2 and runs the KDP between B and A_2. B observes that the SPs of A_1 and A_2 are the same. So, they can be both marked as Sybil nodes[2]. The main idea is that in the normal case, when there is no Sybil attack, the probability of such an observation is very negligible. The probability is calculated as follows:

$$Pr_1 = Pr\ \{(K_{A1} \cap K_B) = (K_{A2} \cap K_B)\ \&\ |K_{A1} \cap K_B| > q\} = \sum_{x=q}^{m} \frac{\binom{m}{x}\binom{P-m}{m-x}}{\binom{P}{m}} \times \frac{\binom{P-m}{m-x}}{\binom{P}{m}} \quad (1)$$

Numerical illustration shows that the above probability is negligible for typical values of P, m and q. For example, if we set P = 10, 000, m = 120 and q = 2, which leads to pc = 0.42, the above probability is 9×10^{-6}. As seen in Fig. 1, for P=2000 and 60 keys stored at each sensor, the probability is less than 1.6×10^{-3}. Therefore, it is highly unlikely that this could be the normal case, and B could easily identify the potentially Sybil nodes in the case of strategy 1.

Following the identification of the set of the potential Sybil nodes S, a resource testing approach can be followed including B and nodes in S. A more aggressive approach from B could be the exclusion of the nodes included in S, from the list of trusted neighbors. In the first case, there is an obvious benefit in terms of power consumption compared to the classical resource testing approaches, given the limited set of nodes to test. The latter approach can be followed when the number of secure links to other nodes approximates the number of expected neighbors for B.

---

[2] *B can finish the protocol here and consider A_1 and A_2 as Sybil nodes. But, there is a very low probability for an error. To be sure, he can now start a resource testing protocol only with the marked neighbors.*

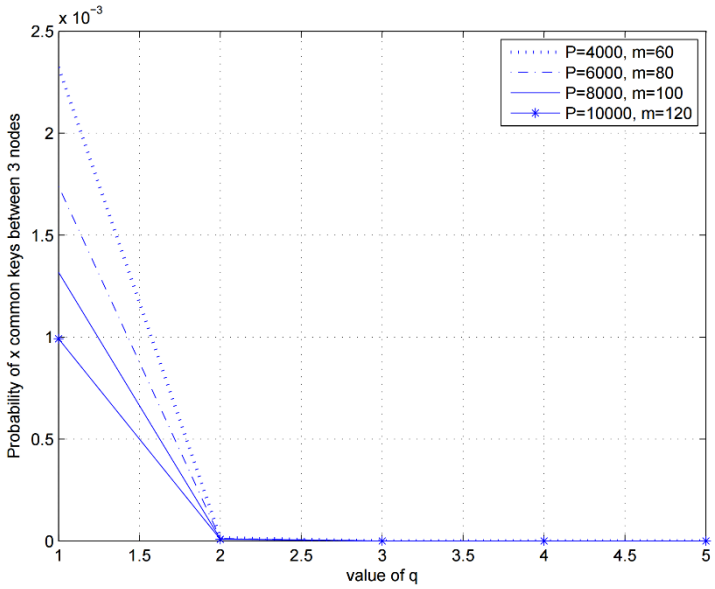

Fig. 1. Naive attacker strategy

B. Strategy 2: Present the subsets of the common keys strategy

In order to avoid easy detection, the attacker could present a subset of the discovered common keys with B, after following the KDP. When A_1 runs the KDP with B, she may figure out that she has more than q common keys with B. In this case, she can choose a subset of the common keys with B, at least q of them, and create a new key ring for the second adversarial node, containing the common keys as well as some dummy keys (or non-shared keys). Then, A_2 runs the KDP with B and tries to establish a secure link. But, B can observe that the SP_{A2} is a subset of SP_{A1}. This is not a normal case, because the probability of such event is very low. We calculate the probability of a set of common keys between B and A_2, to be a subset of the common keys between B and A_1 as:

$$Pr_2 = Pr\{(K_B \cap K_{A2}) \subseteq (K_B \cap K_{A1}) \,\&\, |K_B \cap K_{A2}| > q \mid |K_B \cap K_{A1}| = x\} = \sum_{y=q}^{m} \frac{\binom{x}{y}\binom{P-m}{m-y}}{\binom{P}{m}} \quad (2)$$

For a numerical illustration, we set P = 5000, m = 100 and q = 2, which leads to pc = 0.6. For x = 4 (B shares four keys with A_1), i.e. occurred with probability 0.14, the above mentioned probability is only 3×10^{-4}. While the above probability is 0.002 for x = 8 (and may be not negligible), the probability that x = 8 occurs is only 8×10^{-4} and could be ignored.

Fig. 2 demonstrates the above probability for different values of q, and x shared keys between B and A_1. We observe that for greater values of q, pr_2 is dropping, and for q > 3 is less than 1%. Essentially, this means than for q=2, a sensor with 40 neighboring nodes, would not expect any nodes to have the same profiles.

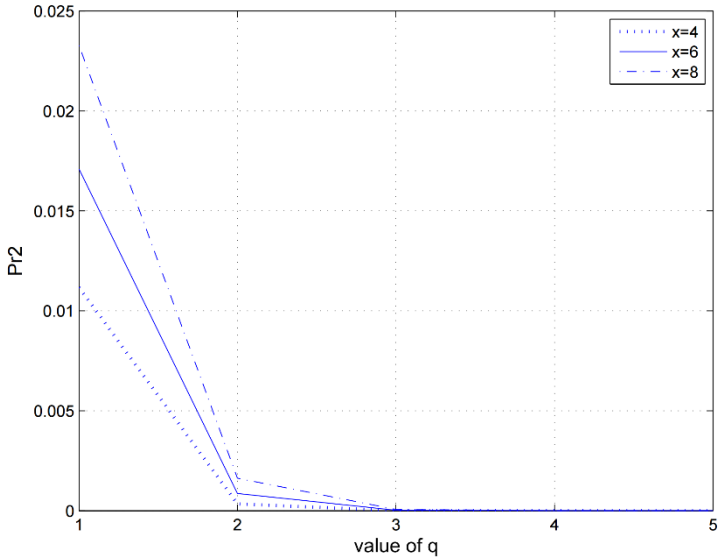

Fig. 2. Probability of SP_{A1} to be a subset of SP_{A2} Profile

C. A Smart Adversarial strategy

In this case, we deal with a smart attacker, who knows about our defense. So, she does not run KDP with all of her keys together (at the same time). Instead, she splits her key set into 2 parts. A_1 and A_2, each one inherits one part of key set. They complete their key sets with self-generated dummy keys. Then, they follow KDP with B. This way the attacker assumes, but doesn't know a priori, that the two parts will have at least q common keys with B to start a connection. The adversary succeeds if A_1 and A_2, each one has at least q common keys with B. The probability of a successful attack is:

$$Pr_3 = \{|K_B \cap K_{A1}| > q \;\&\; |K_B \cap K_{A2}| > q\} =$$

$$\sum_{z=q}^{m/2} \sum_{y=q}^{m/2} \Pr\{|K_B \cap K_{A1}| = z \;\&\; |K_B \cap K_{A2}| = y\} =$$

$$\sum_{z=q}^{m/2} \sum_{y=q}^{m/2} \Pr\{|K_B \cap K_{A1}| = z \times \Pr\{|K_B \cap K_{A2}| = y \mid |K_B \cap K_{A1}| = z\} =$$

$$\sum_{z=q}^{m/2} \sum_{y=q}^{m/2} \frac{\binom{m}{z}\binom{P-z}{m/2-z}}{\binom{P}{m/2}} \times \frac{\binom{m-z}{y}\binom{P-\frac{3}{2}m+z}{m/2-y}}{\binom{P-m/2}{m/2}} \quad (3)$$

Fig. 3 shows the probability of a successful strategy three attack. While this probability is not negligible (i.e. q = 1), the adversary can generate only one extra node in this way. The Increase of the value of q parameter, decreases the probability that the adversary will successfully introduce two Sybil identities.

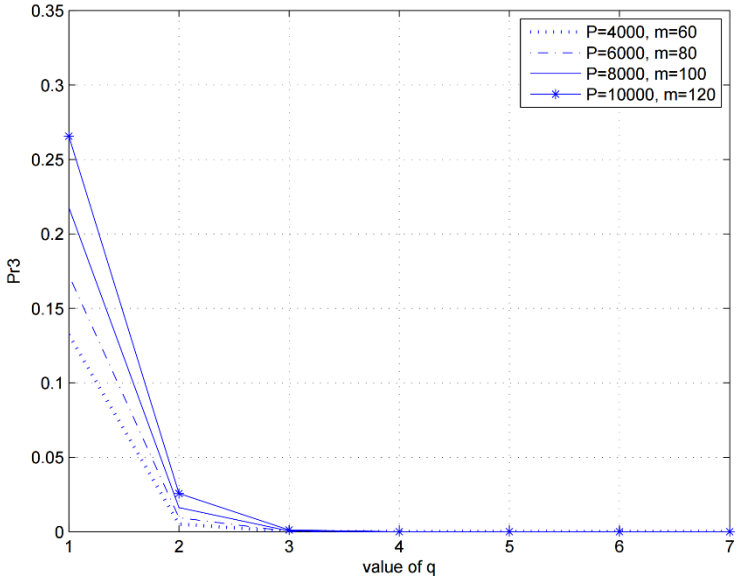

Fig. 3. Probability of a successful strategy three attack

However, we consider this case as the least harmful one, since only two identities are created. If the adversary wants to create more Sybils, she should follow one the previous strategies, after following strategy 3. As shown above, it is easy to detect such attempts. However we present this strategy as an introduction to strategy 4.

D. Strategy 4: Getting Even Smarter

In this case, the attacker does not run the KDP with B, with all of her keys. Instead, she creates lots of nodes such that each key set inherits part of original key set (at most q of them) plus some dummy keys. As an example, the attacker can split her key set into m parts such that each part has only one real key and complete each part with m − 1 dummy keys. Then, each part starts the KDP with B. In this way, none of the adversarial nodes can establish a connection with B (if q > 1). But, all of the shared keys between adversary and B are revealed to the adversary in a stealthy manner. We stress out here, the importance of the KDP scheme. If the list of key indexes is N's key ring are broadcast in clear text [4], the adversary can only run the KDP once. This will provide all the information needed to plan the attack. After that, she can create some Sybil nodes such that each node owns at least q common keys with B. If adversary observes that she has x common keys with B, she can generate $\binom{x}{q}$ key rings such that none of them is equal or a subset of another one (passing our defenses against Strategy 1 and Strategy 2).

D.1. How can we defend against Strategy 4?

The union of my shared keys with my n neighbors has at least n×q keys if there is no overlap between them. It seems that usually there is a "low" overlap between them. So, the union has at least n×q keys or a little below this number. If we observe that the number of keys in the union is too less than n×q, it might be a Sybil attack. We discuss about this defense in the future works.

E. How many Successful Sybil Identities?

We assume a certain network density for the network. Each sensor has an expected number of neighbors, n′. For our calculations we assume that n′ is 40 or 60. We calculate the probability of two nodes sharing x keys as:

$$\Pr_4\{\text{Two Nodes Share x}\} = \frac{\binom{m}{x}\binom{P-m}{m-x}}{\binom{P}{m}} \quad (4)$$

We can then calculate the expected node degree, which is the number of secure links that a node can establish with its neighbors.

$$d = \Pr_4(x) \times n' \quad (5)$$

We define a successful Sybil identity, as the fabricated Sybil identity that can go undetected by our scheme. The maximum number of successful Sybil nodes that can be introduced, given a smart adversary of strategy 4, can be computed as:

$$\sum_{x=q}^{m} \binom{x}{q} \times Pr_4(x) \quad (6)$$

where Pr(x) is the probability that two sensors share x keys.

Fig. 4 demonstrates the expected number of successful Sybils and sensor degree. The attacker can successfully introduce only a small number of successful Sybil nodes in the network. Moreover, the number of successful Sybil is extremely low, compared to the number of expected neighbors. Therefore, if the attacker was targeting a WSN service that requires redundancy, or requires a majority of honest nodes, the attacker would be rather unlikely to succeed. For example, a sensor reputation system, should be able to operate using our scheme, and it should be protected against Sybil attacks.

IV. RELATED WORKS

Resource testing techniques, social networking approaches, and trusted certification are the Sybil attack countermeasures proposed in literature. As noted in the previous sections, scarce sensor resources limit the applicability of the proposed solutions. In this section we present the most important of the related works, and do not perform a full range survey of the literature.

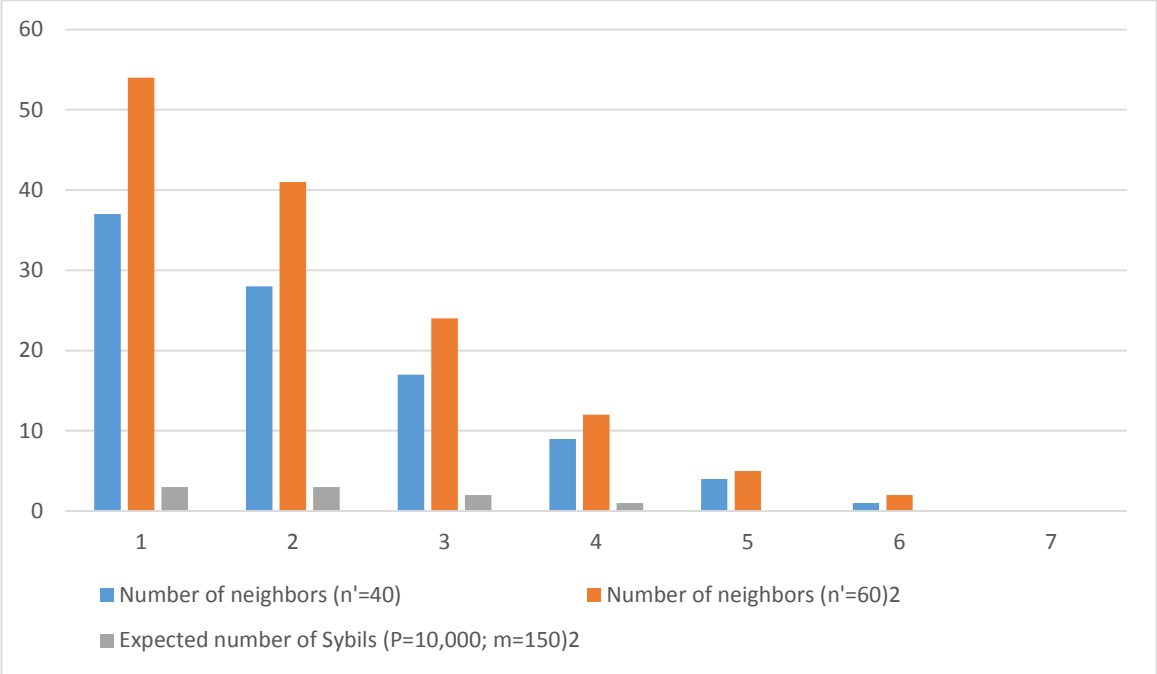

Fig. 4. Number of successful Sybil identities introduced

Resource testing techniques in sensor networks, challenge neighboring nodes and verify their physical existence with the use of computational puzzles. The verifying node challenges its neighbors simultaneously to solve the cryptographic passwords and reply within a time frame, which is defined by the password's complexity and affected by the sensors' location. Responses that arrive after the expiration of the response deadline are discarded, and the nodes that fail to provide the answer are considered Sybils.

The main idea of resource testing, is that one adversarial node pretending to be many Sybil identities, cannot answer for all of them given the limited resources of a neighbor and the time limit set by the verifier. It is obvious though that resource testing techniques for WSN consume a lot of resources due to the expensive computations involved and the necessary exchange of messages. However, our scheme can act as an important extension to resource testing, since it limits the number of nodes to verify, or equivalently, creates a limited set of potentially Sybil nodes. A formal analysis of secure neighbor discovery, which is also important to launch the resource testing schemes, is studied in [9], [10]. Secure sensor location in sensor networks important for the computation of the time-of-flight has been studied in [11], [12]. Radio testing which was proposed in [7], falls into the same category with resource testing techniques, and will unavoidably have an impact in the sensors' resource consumption. Other researches that consider resource testing techniques include [19] and [24]. Also, [25]-[27] study Recurring Costs, which is a branch of resource testing. Additionally, social networking approaches are not suitable for ad-hoc WSN, and in most cases they rely on centralized infrastructure.

Other approaches include a positioned-based countermeasure, as seen in [28], as well as the Received Signal Strength Indicator (RSSI) method, which is studied in [29]. John et.al. [13] and Balachandran et.al. [17] review several countermeasures against Sybil attack and classified them.

A trusted identification authority is the only means to limit an adversary from introducing Sybil identities in the network, as proven by Douceur in [1]. This method is considered in [20] and [21]. However, this is not a suitable solution for WSNs, because of the cost introduced by public key cryptography. In [22] Sybil Infer is studied, which is a central approach, too. Pairwise key distribution schemes, apply node authentication by associating a sensor identity to a unique key, using symmetric crypto, but unavoidably limit the size of the supported network. Each sensor shares one unique common key with exactly m other nodes, where m is the size of the key ring. Therefore, each sensor can establish a secure link with at most m nodes [7]. The size n of the network can be computed as n = m/p, where p is the probability that any two nodes are connected. To increase the supported network size, a multi-hop range extension is proposed [7]. However, the sensor ID re-broadcast mechanism of the scheme used to reach nodes that are not in the vicinity of a sensor, is done via a non-authenticative manner. This allows an adversary to launch DoS attacks, especially for the case of colluding adversaries that can collect multiple network identities and flood the network with requests [3]. But in this approach, the re-broadcast of the sensor IDs is done without authentication, which can create serious security vulnerabilities with DoS attacks [3]. Therefore the pairwise scheme is not suitable for a large variety of applications, unless flexibility, node additions and limited network size are not an issue. The supported network size is much smaller compared to the basic and the q-composite schemes.

There are several more researches that consider RKD to resist against Sybil attack, none of them uses a currently known scheme like q-composite. According to our best knowledge, most of them introduces a new RKD to improve network resilience against Sybil attack. For example, [15] explains a location-based RKD. Newsome et.al. [19] explain Key Validation Test for random key predistribution. They use a special form of basic scheme that keys are assigned to nodes according to a Pseudo-Random Function. It is a challenge-response method that each node should prove owning the claimed keys. Unlike our approach, this method discharges network resources. Besides, our approach can be used when the challenge-response test is passed by nodes.

Moore in [16] analyzes [19] and mount an attack to it. Moore shows that [19] is vulnerable against the proposed attack. Finally, he suggests Secure Path Key Revocation to resist against the attack.

[23] proposes a location-aware RKD to stand with Sybil attack. In [14], if a node claims owning a key, that key should exist in the key pool. Also, [18] introduces a new RKD to mitigate the risks of Sybil attack.

V. SUMMARY

In this work we proposed a Sybil detection mechanism that improves the resilience of large WSNs against a variety of adversarial strategies. By applying our method to the q-composite scheme, we are able to support large sensor networks, and minimize the effects of a Sybil attack. We prove this by showing that the number of potentially undetected nodes, is much smaller than that expected number of legitimate neighbors. This makes the attack unsuccessful against its common targets, such as voting schemes that require the majority of the malicious nodes. For future work we plan to extend our analysis for more advanced adversarial strategies, such as the case of the colluding adversarial nodes. We want to test the efficiency of our scheme against those and propose an enhanced defense.

REFERENCES

[1] J. R. Douceur, “The Sybil attack,” in Revised Papers from the First International Workshop on Peer-to-Peer Systems, London, UK, 2002, pp. 251–260.

[2] Q. Wang, Y. Zhu, and L. Cheng, “Reprogramming wireless sensor networks: challenges and approaches,” IEEE Network, vol. 20, no. 3, pp. 48–55, 2006.

[3] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in Proceedings of the 2003 IEEE Symposium on Security and Privacy, Washington, DC, USA, 2003, pp. 197–213.

[4] 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, 2002, pp. 41–47.

[5] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A pairwise key predistribution scheme for wireless sensor networks,” in Proceedings of the 10th ACM conference on Computer and communications security, 2003, pp. 42–51.

[6] D. Liu and P. Ning, “Establishing pairwise keys in distributed sensor networks,” in Proceedings of the 10th ACM conference on Computer and communications security, 2003, pp. 52–61.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil attack in sensor networks: analysis & defenses,” in Proceedings of the 3rd international symposium on Information processing in sensor networks, 2004, pp. 259– 268.

[8] P. Papadimitratos and J. Deng, “Stealthy pre-attacks against random key pre-distribution security,” in Proceedings of the IEEE International Conference on Communications - Communication and Information Systems Security Symposium (ICC’12 CISS), Ottawa, Canada, 2012, pp. 251–260.

[9] M. Poturalski, P. Papadimitratos, and J.P. Hubaux, “Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility,” in ACM Symposium on Information, Computer and Communications Security (ASIACCS), Tokyo, Japan, March 2008, pp. 189–200.

[10] M. Poturalski, P. Papadimitratos and J.P. Hubaux, “Towards provable secure neighbor discovery in wireless networks,” in ACM Workshop on Formal Methods in Security Engineering, Alexandria, VA, USA, October 2008, pp. 31–42.

[11] Y. Zhang, W. Liu, Y. Fang, and D. Wu, “Secure localization and authentication in ultra-wideband sensor networks,” Selected Areas in Communications, IEEE Journal on, vol. 24, no. 4, pp. 829 – 835, April 2006.

[12] D. Liu, P. Ning, and W. Du, “Detecting malicious beacon nodes for secure location discovery in wireless sensor networks,” in Distributed Computing Systems, 2005. ICDCS 2005 Proceedings. 25th IEEE International Conference on, June 2005, pp. 609–619.

[13] R. John, J.P. Cherian, and J.J. Kizhakkethottam, "A survey of techniques to prevent Sybil attacks", in Soft-Computing and Networks Security (ICSNS), 2015 International Conference on, IEEE, 2015, pp. 1-6.

[14] R. Gunturu, “Survey of Sybil Attacks in Social Networks,” arXiv preprint arXiv:1504.05522, 2015.

[15] M.M.M. Fouad, and A.E. Hassanien, "Key Pre-distribution Techniques for WSN Security Services," in Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations, pp. 265-283. Springer Berlin Heidelber, 2014.

[16] T.W. Moore, "Cooperative attack and defense in distributed networks," Doctoral dissertation, University of Cambridge, 2008.

[17] N. Balachandran, and S. Sanyal, "A Review of Techniques to Mitigate Sybil Attacks," International Journal of Advanced Networking and Applications, vol. 4, no. 1, pp. 1514-1518, 2012.

[18] C. Cheng, Y. Qian, and D. Zhang, "An Approach Based on Chain Key Predistribution against Sybil Attack in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 839320, 8 pages, doi:10.1155/2013/839320, 2013.

[19] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," Proceedings of the 3rd international symposium on Information processing in sensor networks, pp. 259-268, 2004.

[20] B. N. Levine, C. Shields, and N. B. Margolin, A survey of solutions to the Sybil attack, University of Massachusetts Amherst, Amherst, MA, 2006.

[21] L. Washbourne. A Survey of P2P Network Security, arXiv:1504.01358, 2015.

[22] W. Chang and J. Wu, "A Survey of Sybil Attacks in Networks," in publications of computer and Information Sciences, Temple University, Philadelphia, 2013.

[23] Zhao, H., Li, Y., Shen, J., Zhang, M., Zheng, R., Wu Q., "A New Secure Geographical Routing Protocol Based on Location Pairwise Keys in Wireless Sensor Networks," 2013.

[24] G.V. Rakesh, S. Rangaswamy, V. Hegde, G. Shoba, "A Survey of techniques to defend against Sybil attacks in Social Networks," in IJARSCCE, 2014.

[25] B. Awerbuch and C. Scheideler. Group Spreading, "A Protocol for Provably Secure Distributed Name Service," in Proc. Automata, Languages and Programming (ICALP), pp. 183–195, 2004.

[26] P. Maniatis, D. S. H. Rosenthal, M. Roussopoulos, M. Baker, T. Giuli, and Y. Muliadi, "Preserving peer replicas by ratelimited sampled voting," in Proceedings of ACM SOSP, pp. 44–59, 2003.

[27] P. Maniatis, M. Roussopoulos, T. J. Giuli, D. S. H. Rosenthal, and M. Baker, "The locks peer-to-peer digital preservation system," ACM Transactions on Computer Systems, vol. 23, no. 1, pp. 2–50, 2005.

[28] A. Tangpong, G. Kesidis, Hung-yuan Hsu, A. Hurson, "Robust Sybil Detection for MANETs," In Proceedings of 18th International Conference on Computer Communications and Networks, ICCCN 2009, pp. 1-6, 2009.

[29] M. Demirbas, Y. Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," in Proceedings of WoWMoM 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006.