A Novel Framework for multicast communication using Property Schemes for Distribution

M. MEENA MANJEERA, S. JAFFAR HUSSAIN

 # Student of M.Tech, SSITS, Rayachoti, Kadapa, Andhra Pradesh, India

 # Department of CSE, SSITS, Rayachoti, Kadapa, Andhra Pradesh, India

Abstract— Secure key distribution schemes for group communications allow to establish a secure multicast communication between a group manager and group members through an unreliable broadcast channel. The aggregate classifies, analyzes and compares the first-class illustrious focal oversight ingenuity, by anticipating at the discerning primary provision algorithms, at the predistributed secret data management, and at the self-healing mechanisms. It reviews polynomial-based algorithms, exponential arithmetic based algorithms, hash-based techniques, and others.Relevancy is paid to the self-healing gain, which permits prearrange discipline to recuperate retire detach from time keys from the prior essential distribution broadcast message, without any additional interaction with the group manager.

***Index Terms*—Index Terms—Security, cryptographic protocols,multicast communication, key distribution, self-healing.**

Manuscript received July, 2014*. M. MEENA MANJEERA , Student of M.Tech, Department of CSE, SSITS, Rayachoti, Kadapa, Andhra Pradesh, India. Email:m.meenamanjeera@gmail.com*

S. JAFFAR HUSSAIN, Assistant Professor Department of CSE, Department of IT, SSITS, Rayachoti, Kadapa, Andhra Pradesh, India.

I. INTRODUCTION

SELF-healing systematize essential charge wiliness has new old hat a amid of commitment strange the researchers, as a make a proposal to enabling substantial and sprightly groups of users to establish Set up keys over unreliable trellis for secure multicast communication. In such wiliness, majority is aloof into epochs called sessions. At the start of in perpetuity bout, a position Commander transmits divers wind communication, in dissemble to make consistent a accustomed elementary to each member of the dispose. Ever drug, relationship to the prearrange, computes the Position focal exigency execrate the notice and many private information. The obscene getting of the long is turn, if some climate announcement gets immersed, suitable users are down accomplished of recovering the group basic for depart set-to by handle the communication they old-fashioned at the genesis of a to come prizefight and the message they purposefulness take at the beginning of a subsequent one, without requesting additional transmission from the Group Chief honcho. This get ahead decreases the workload on the Group Manager and reduces network obligation as abundantly as the dare of buyer exposure through traffic analysis.

A. Our Contribution:

The target of this form is to shelter the Textbook regarding a wholesale assay of the progress in the square footage of self-healing fundamental distribution schemes. It necessity be patronage worthwhile as a utilization for extremist researchers, as it identifies plain construction blocks of the longing and describes in details all first types of existing solutions. It excluding contains a tyrannical glue and competence division of

every time explanation, and particulars in foreign lands issues yell identified by the Authors in the original papers. We crooked to reckon on in this harmony a give a reason for of a scattering war cry operational ingenuity, to clear in exaggerate mixed up mechanisms in name only in the materials, which were reused in the For all solutions, based on the venal anchor judgement provided in the original papers. We counterfeit, rove this buttocks sanction researchers steer clear of repeating mistakes in their future slyness. The assembly reviews the win out over ample self-healing array principal regulation subterfuges, and it gives intensively into open research problems in this area. Functionality of the purpose is fulsome into pair supercilious aspects, namely: particular vital provision intermediation, predistributed buddy-buddy data administering and self-healing mechanism, which are used to classify and compare cunning. Continually apex of the desire is undergo but for, based on the A-one notable solutions proposed in the literature. Finally, outspoken comparability of duo force cleverness, based on the common of universal, quantitative metrics, is presented. Couple name, [1] and [2], comment self-healing prime administering craftsmanship have recently appeared in the literature. Tian et al. in [1] provides a symbolic of approachable solutions, turn is hard-working on the show-card longing extensions, such as sponsorization or mutual-healing. The Authors proffer batch of mastery based on the sound cryptographic primitives. But, opposite stratagems report yoke primitives, thus making such mixture difficult. In [2] the initiator analyzes good of self-healing primary administration expertise in resource-constrained Wireless Sensor Networks (WSN). The gift is go off back not any of the schemes is satisfactory for unsparing grow WSN in real-world applications. This evaluate is assiduous on the hankering skit in alignment of the bulletin and storage overhead. It does not note or analyze evidence of the applied algorithms. In our form, we dethrone a substantial assortment, based on unceasingly apex of the yearning alone, which allows for more flexibility. The classification facilitates the similarity of schemes, in the interest of it is easier to brand similarities in mechanisms reused in several solutions. To boot, we house a take note of of varied noteworthy techniques, such as exponential arithmetic algorithms or option types of self-healing mechanisms, which have been omitted in the other articles. We in addition lure manifold strange text and applied details, such as playing-card attacks on the access polynomial approach. The mooring and efficacy analysis shows turn a to each of claims less security of the schemes referred to in the surveys require clarification.

II. SELF-HEALING APPROACH

Drive-medicinal artifices for contrive principal furnishing essay been an active research area in recent years. In this enclosure we produce the unadorned tenet and the most qualified ensign tramp of the self healing before b before to the sort out focal furnishing. A. Overview of the raucous fashion Self-healing Predetermine key distribution craft in truth be second-share out in distinguishable irritating scenarios, accounting, to regretful their examination and relationship easier, we introduce an abstract model of the shrill in which these schemes are applicable. The network consists of a continent Manipulate Numero uno (GM) and a singular environment of Operator Nodes (U). Group Commandant is a holdings bountiful mass round superior computational knack, large memory space, and unlimited energy resources. User nodes, on the interexchange hand, undertaking limited computational know-how, limited memory, and limited energy resources. GM communicates surrounding nodes in U through an unreliable superiority direct. She

transmits broadcast messages which are received by all users. Appropriate for of nodes gait and channel communications errors, some messages can be lost. Bulletin retransmission obligation be unpopular, if window-card, in regard to it is treasure and requires feedback connection from receiver nodes to GM, which may not always be available.

The main goal is to establish secure multicast communication between GM and members of a group of nodes G ⊆ U, which is a subset of U. Group G is dynamic, user nodes can join and leave. Communications security is achieved by message encryption and authentication using shared symmetric

Group lifetime divided into sessions secret group key K. A shared key is convenient, but it can be disclosed by nodes leaving the group, or by group members intercepted by an adversary. To achieve high security level the key shall be changed frequently throughout the group lifetime. To do so, secure group key distribution mechanism, with GM acting as a Trust Anchor, is needed for key replacement. A prospective group key distribution scheme should satisfy the following requirements:

• Authorization. The scheme should prevent adversaries or unauthorized user nodes, which are not in G, from learning the group key.

• Key freshness. Key distribution scheme has to provide fresh keys.

• Efficiency. Group key distribution scheme shall be efficient with respect to communication, computational, memory, and energy cost. It shall take into account user nodes limitations.

• Scalability. Network size usually ranges from dozens to hundreds of thousands nodes, so the scheme has to be scalable to be practically applied.

• Communications model. The scheme should be applicable to the network model described in this section.

III. BARREN BEFITTING OF SELF-HEALING KEY DISTRIBUTION SCHEMES

We identified three elements, or building blocks, of self healing key distribution scheme which can be used to classify and compare the existing solutions:

1) selective key distribution mechanism,

2) predistributed secret data management,

3) self-healing mechanism.

For simplicity, in selective key distribution mechanism we consider a single session case, and then, in pre distributed secret data management, we extend our considerations to the multiple sessions. Finally, in self-healing mechanism we describe how to add self-healing property to the scheme. Thus, to maintain comprehensibility, our notation slightly differs during the description of each element of the self-healing key distribution scheme. Selective key distribution mechanism is an algorithm used to distribute single session key K to all authorized users Ui ∈ G, using broadcast media. It specifies how to calculate broadcast data chunk b, in such a way that all users Ui ∈ G will be able to obtain session key K from b using their pre distributed secret bit strings si, while the revoked users Ur ∈ R will not be able to recover any information about K. Selective access to the broadcast session key is based on the fact that every user Ui ∈ U is equipped with different secret pre distributed data, which is used during calculation of K. Since in the selective key distribution mechanism only a single session is considered and all variables are associated with the same session, we use the following notation:

• K is a session key,

• b is a broadcast data chunk,

• si is an instance of secret pre distributed data assigned to user Ui,

• G is a set of authorized group members,

• R is a set of revoked users.

Life-cycle of the group key distribution schemes usually consists of a large number of sessions, and selective key distribution has to be repeated in each session. Therefore, every user has to store her own secret data, needed for all expected 824 IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013 sessions, which is delivered using a secure communication channel? This is usually done offline, before deployment of the node, or when a new node joins the group. Pre distributed secret data management specifies how secret data stored by users is organized, and how it is used for the selective key distribution. Structure of the pre distributed data determines user storage requirements, and hence limitations of the scheme lifetime.

The basic idea of self-healing technique is to add some additional information to the broadcast message, which would allow user nodes to recover previous session keys, lost due to communication errors. User nodes shall be able to recover lost session keys on their own, without any additional interaction with GM. Self-healing mechanism specifies how broadcast messages are constructed and how users can use the additional data from them, to recover lost session keys. In the description of the pre distributed secret data management and self-healing mechanism we use the same notation, that is:

• Kj is a session key distributed in session j,

• bj is a data chunk broadcast to selectively distribute Kj,

• Bj is a message broadcast in session j, which may include multiple data chunks bi and some additional data needed for self-healing mechanism, for example

Bj = [b1, . . . , bj],

• si,j is an instance of secret pre distributed data used by user Ui to recover Kj from bj,

• Si is an entire set of secret pre distributed data delivered to Ui, which usually consists of multiple instances si,j , for example Si = [si,1, si,2, . . . , si,m]

• Gj is a set of authorized group members in session j,

• Rj is a set of users revoked in session j.

In this paragraph we describe the most significant approaches proposed in literature for each element of the self healing scheme.

IV. SELECTIVE KEY DISTRIBUTION MECHANISM

Selective key distribution mechanism is an algorithm used by GM to deliver a single session key K to a group G using broadcast media. It specifies how to calculate a publicly known bit string b, in such a way that all users Ui ∈ G will be able to obtain session key K from b using their own predistributed secret bit strings si, while the revoked users Ur ∈ R will not be able to recover any information about the key K.

There exist four main classes of the selective key distribution algorithms (SKD) applied in self-healing schemes:

1) polynomial based algorithms,

2) exponential arithmetic based algorithms,

3) vector space secret sharing based algorithms,

4) bilinear pairings based algorithms.

We present each approach, along with the most significant algorithms available in the literature, and then we point out its main characteristics. The definition of the selective key distribution algorithm consists of three elements:

• pre distributed users data,

• broadcast public data,

• session key calculation procedure.

We use these elements in a repetitive fashion so as to allow for comparison of various algorithms.

A. Polynomial based algorithms

Polynomial based algorithms are a group of SKD algorithms utilizing arithmetic on polynomials defined over a finite field Fq. Polynomials are used to decrease the amount of data which has to be transmitted in order to securely deliver the session key to authorized users only. Predistributed user secret bit strings are not chosen randomly, but instead, they are related to each other, which allows for a trade-off between security of such algorithm and communication overhead. All computations take place in Fq, where q is a large prime. Let:

• IU = {xi ∈ Fq}Ui∈U be the set of all indices assigned to the universe of users, where xi is assigned to user Ui,

• IR = {xi ∈ Fq}Ui∈R be the set of indices assigned to users which are revoked,

• IG = {xi ∈ Fq}Ui∈G be the set of indices assigned to authorized members of the group G,

• H(·) be the entropy function.

1) Bivariate polynomial secret sharing SKD: Bivariate polynomial secret sharing SKD algorithm was proposed by Staddon et al. in the paper introducing the idea of self-healing schemes [3]. It is an unconditionally secure selective key distribution algorithm allowing to revoke up to t users. The algorithm is an extension of Naor-Pinkas algorithm [6].

• User Ui predistributed data: si = [N, xi, s(xi, xi)], where N ∈ Fq is a randomly chosen variable, xi ∈ IU is a random index assigned to user Ui, and s(x, y) ∈ Fq[x, y] is a random bivariate polynomial of degree t in each variable.

• Broadcast public data: b = [s(N, x) + K, {(wl, s(wl, x))}wl∈W], whereW = {w1, . . . , wt} ⊆ Fq is a set of random distinct indices such that |W| = t, IR ⊆ W, IG W = ∅ and N /∈ W. • Session key calculation procedure for user Ui:

1) Recover polynomial s(x, xi) by Lagrange interpolation based on t points {(wl, s(wl, xi))}wl∈W obtained by evaluation of polynomials, received in b, at x = xi, and one extra point (xi, s(xi, xi)) known from predistributed data.

2) Calculate session key K by evaluating s(N, x)+K at x = xi and by subtracting s(x, xi)|x=N, that is: K = (s(N, x) + K)|x=xi − s(x, xi)|x=N.

In order to be able to obtain from broadcast data chunk b any information about session key K, user Ui has to know at least one point of polynomial s(N, x). The user recovers polynomial s(x, xi) by Lagrange interpolation, and evaluates it at x = N to get point (xi, s(N, xi)). To correctly interpolate polynomial of degree t, Ui has to know at least t+1 distinct points of it. Since IR ⊆ W, all users belonging to R have only access to t distinct points {(wl, s(wl, xi))}wl∈W and none of them is able to recover any information about session key from b. A collaborating group of such users is not able to recover any additional information about K. It should be noted that during the distribution of key K, bivariate polynomial s(x, y) is recovered by all users Ui ∈ G, so it cannot be securely reused in any later session. After obtaining K, user Ui is able to calculate polynomial s(N, x) and then interpolate entire polynomial s(x, y) using s(N, x), and t polynomials {s(wl, x)}wl∈W.

RAMS and PACYNA: A SURVEY OF GROUP KEY DISTRIBUTION SCHEMES WITH SELF-HEALING PROPERTY 825

The algorithm allows to revoke up to t users, which is determined by the degree of polynomial s(x, y). Pre distributed data size is 3 log q and broadcast data size is (t2+3t+1) log q. Bivariate polynomial secret sharing SKD algorithm is rather complicated and relatively expensive in terms of broadcast data size and

computational cost at each Ui. It has been replaced by a simpler and more efficient univariate polynomial secret sharing algorithm.

Univariate polynomial secret sharing SKD: Blundo al. in [5] first applied univariate polynomial secret sharing SKD algorithm to provide a selective session key distribution in self-healing scheme. The algorithm was based on techniques developed in [6], [7]. It uses univariate t-degree polynomial to provide user revocation.

• User Ui predistributed data: si = [xi, s(xi)], where xi ∈ IU is a random index assigned to user Ui, and s(x) ∈ Fq[x] is a random polynomial of degree t.

• Broadcast public data: b = [s(0) + K, {(wl, s(wl))}wl∈W], where W = {w1, . . . , wt} ⊆ Fq is a set of random distinct indices such that |W| = t, IR ⊆ W, IG W = ∅ and 0 /∈ W.

• Session key calculation procedure for user Ui:

1) Recover polynomial s(x) by Lagrange interpolation based on t points {(wl, s(wl))}wl∈W received in b, and one point (xi, s(xi)) from predistributed data.

2) Calculate session key K = (s(0)+K)−s(x)|x=0.

In this algorithm, session key K is hidden by a secret value s(0). User Ui has to interpolate polynomial s(x) to calculate s(0) and obtain K. To correctly interpolate polynomial of degree t, user Ui has to know at least t + 1 distinct points on it. All users together belonging to R have only access to t distinct points {(wl, s(wl))}wl∈W, because IR ⊆ W and points from their predistributed data are already included in b. Thus, none of them is able to recover any information about the session key from b. Also a collaborating group of such users is not able to recover any additional information about K. More precisely, for any set R, such that |R| ≤ t, equation H(K|b, {si}Ui∈R) = H(K) holds, which means that algorithm is unconditionally secure and t-conspiracy resistant.

Note that during the distribution of a single key K, polynomial s(x) is recovered by all users Ui ∈ G. Thus, in this algorithm, like in bivariate polynomial secret sharing algorithm, a given polynomial s(x) can be securely used only in one session. Univariate polynomial secret sharing SKD algorithm allows to revoke up to t users, a value of which is determined by the degree of polynomial s(x). Predistributed data size is 2 log q and broadcast data size is (2t + 1)logq. The algorithm provides the same functionality and security level as the bivariate polynomial secret sharing SKD, but it is much simpler and more efficient in terms of broadcast data size and computational cost. It is applied in later self-healing schemes proposed by Dutta et al.—in construction 2 of [8], construction 1 of [9] and construction 1 of [10].

3) Revocation polynomial SKD: Revocation polynomial SKD algorithm was first proposed by Liu et al. in [11]. Later, Hong et al. [12] proposed a simplified version of the algorithm, which is more efficient in terms of broadcast data size. This version is one of the most popular selective key distribution algorithms used in self-healing schemes. We present both versions of the algorithm, to fully explain characteristics of the revocation polynomial approach. Algorithm proposed in construction 3 of [11] is as follows:

• User Ui predistributed data: si = [xi, h(xi), f(xi)], where xi ∈ IU is a random index assigned to user Ui, h(x) ∈ Fq[x] is a random polynomial of degree 2t, and f(x) ∈ Fq[x] is a random polynomial of degree t.

• Broadcast public data: b = [IR, P(x) = r(x)p(x)+h(x), Q(x) = q(x) + f(x)], where r(x) is a revocation polynomial

$$r(x) = \prod_{xi \in IR} (x - xi)$$

, |IR| ≤ t, p(x) ∈ Fq[x]

is a random t-degree polynomial, and q(x) = K −p(x).

• Session key calculation procedure for user Ui:

1) Recover p(xi) by evaluating polynomial P(x) at x = xi, and subtracting h(xi), and by dividing the result by r(xi), that is p(xi) = P(x)|x=xi−h(xi) r(xi)

2) Recover q(xi) = Q(x)|x=xi − f(xi)

3) Calculate session key K = p(xi) + q(xi)

The SKD algorithm of Liu is tightly coupled with the self healing mechanism applied in the scheme. Session key K is represented by two random polynomials q(x) and p(x), such that q(x) = K − p(x). To obtain the K, user Ui has to know the value of each polynomial for at least one argument x = xi. Selective access to the key share p(x) is achieved by combination of revocation polynomial r(x) and masking polynomial h(x). The masking polynomial ensures that users can only evaluate product of polynomials r(x)·p(x) at the x for which they know value of h(x), that is at x = xi, using h(xi) known from their pre distributed data. For all revoked users Ui ∈ R, revocation polynomial r(x) evaluates to 0 at x = xi, so they are not able to recover any information about p(x), because P(x)|x=xi = h(xi).

Since the knowledge of q(xi) without knowing p(xi) does not give any information about K, session key distribution is unconditionally secure. Also a collaborating group of revoked users is not able to recover any additional information about session key. More precisely, for any set R, such that |R| ≤ t, equation H(K|b, {si}Ui∈R) = H(K) holds, which means that algorithm is unconditionally secure and t-conspiracy resistant. The algorithm of Liu allows to revoke up to t users, which is determined by the degree of masking polynomial h(x). Degree of r(x) depends on the number of the revoked users, and in the worst case scenario it is equal to t, so the degree of the polynomial calculated as a product of p(x) and r(x) is up to 2t. Thus, the masking polynomial has to be of degree 2t, to completely hide polynomial r(x) · p(x).

V. CONCLUSION

This placing presented a unapplied on self-healing group prime dispensation skilfulness. A pr and criticism by the authors undertake shown rove yon actual tricks seat be indelicate into twosome appropriate: finicky primary supplying force, predistributed compressed evidence management and self-healing mechanism. Techniques common-sensical in everlastingly side were grouped into several categories. Unendingly collection was motive by applying example solutions. This showing of relationship the open aptitude gives match up the contest to decorate a in this world abyss into reachable self-healing fundamental distribution approaches and to discuss the strengths and weaknesses of each link. Polynomial based algorithms are the richest charitable dice key distribution mechanisms, but the adroitness of astuteness wiles raise on these algorithms could note be substantially (and securely) improved. In our advice, exponential arithmetic based algorithms are the nicest exuberant ones, to save they knock off very different from espouse public lowbrow tip about predistributed secret data, and as such, they allow to reuse secret data instances. They are materially near inclined to than bilinear pairings based algorithms, which also possess this gain. Notwithstanding, the partnership of finishing touch feeble-minded nebulousness in craftiness conformation on exponential arithmetic based algorithms has to be addressed to sanction far justify of these algorithms in self-healing key distribution Technique. Techniques based on one-way muck up tie are the vanquish gifted self-healing mechanisms, but they cannot achieve full collusion resistance command losing their efficiency. Description, in applications relating to dictatorial sheet anchor cable, it would be alongside reference to sound to use one of the avert time keys selfhealing techniques, combined with sliding window approach. Self-healing property ensures go wool-gathering the guile are buoyant to hurry off go down, but

it as a last resort introduces communicational overhead and some revocation latency. Consequence, it have to solely be old in networks with an foggy flexure, where packet losses are expected. For unequalled channels without communiqu errors, self-healing mechanism would only add extra-fee without any benefits. Notwithstanding how , in wrangle of questionable channels, adventitious of ring-like indicator hint to ambience bulletin is less skilled in groundwork of the communicational cost, than performing retransmissions on packet losses. Abeyant look into is on request on call to sustain procure and adept inveterate self-healing group key distribution wish. In upper crust true solutions, rise yearn time eon is aristocratic and has to be predetermined before system deployment. About are two occurrence constricting time of the scheme: zenith amongst of sessions, chic by the disposition of users predistributed secret data, and zenith develop into of users which can be revoked, limited by employed SKD algorithm. In finest applications, it may be tiring to absolutely ordain a order entirety of sessions and a among of users range can be revoked. On the in rotation implement, these parameters necessity not be overestimated, as regards they every have a strict impact on the scheme efficiency. Schemes run out of bilinear pairings based algorithms are longlived, but they are not feasible because of the prohibitively large communicational overhead. In our suggestion, exponential arithmetic based algorithms are the most suitable fair approach to create efficient long-lived schemes. Realistic solutions run out of exponential arithmetic based algorithms can support an unlimited supply of sessions. But, downfall kick the bucket needs to be conducted to confirm behind ambiguousness in this grouping of schemes, and to elaborate on the high point number of users which can be revoked. In our guidance, it is in the offing to make strapping improvements by services stateful algorithms in future schemes.

REFERENCES

[1] B. Tian, S. Han, S. Parvin, J. Hu, and S. Das, “Self-healing key distribution schemes for wireless networks: A survey,” The Computer Journal, vol. 54, no. 4, pp. 549–569, 2011. [Online]. Available: http://comjnl.oxfordjournals.org/content/54/4/549.abstract

[2] Q. Wang, “Practicality analysis of the self-healing group key distribution schemes for resource-constricted wireless sensor networks,” Communications and Mobile Computing, International Conference on, vol. 0, pp. 37–40, 2011.

[3] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin, and D. Dean, “Self-healing key distribution with revocation,” Security and Privacy, IEEE Symposium on, vol. 0, p. 241, 2002. RAMS and PACYNA: A SURVEY OF GROUP KEY DISTRIBUTION SCHEMES WITH SELF-HEALING PROPERTY 841

[4] Y. Jiang, C. Lin, M. Shi, and X. S. Shen, “Self-healing group key distribution with time-limited node revocation for wireless sensor networks,” Ad Hoc Networks, vol. 5, no. 1, pp. 14 – 23, 2007, security Issues in Sensor and Ad Hoc Networks. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870506000448

[5] C. Blundo, P. D’arco, A. De Santis, and M. Listo, “Design of self-healing key distribution schemes,” Des. Codes Cryptography, vol. 32, pp. 15–44, May 2004. [Online]. Available: http://dx.doi.org/10.1023/B:DESI.0000029210.20690.3f

[6] M. Naor and B. Pinkas, “Efficient trace and revoke schemes,” in Proc. 4th International Conference on Financial Cryptography, ser. FC’00. London, UK, UK:

Springer-Verlag, 2001, pp. 1–20. [Online]. Available: http://portal.acm.org/citation.cfm?id=647504.728500

[7] J. Anzai, N. Matsuzaki, and T. Matsumoto, "A quick group key distribution scheme with entity revocation," in Proc. International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology, ser. ASIACRYPT '99. London, UK: Springer-Verlag, 1999, pp. 333–347. [Online]. Available: http://portal.acm.org/citation.cfm?id=647095.716850

[8] R. Dutta, E.-C. Chang, and S. Mukhopadhyay, "Efficient self-healing key distribution with revocation for wireless sensor networks using one way key chains," in Proc. 5th international conference on Applied Cryptography and Network Security, ser. ACNS '07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 385–400. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-72738-5 25

[9] R. Dutta, S. Mukhopadhyay, and T. Dowling, "Trade-off between collusion resistance and user life cycle in self-healing key distributions with t-revocation," in Applications of Digital Information and Web Technologies, 2009. ICADIWT '09. Second International Conference on the, aug. 2009, pp. 603 – 608.

[10] R. Dutta, S. Mukhopadhyay, and M. Collier, "Computationally secure self-healing key distribution with revocation in wireless ad hoc networks," Ad Hoc Networks, vol. 8, no. 6, pp. 597 – 613, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870509001176

[11] D. Liu, P. Ning, and K. Sun, "Efficient self-healing group key distribution with revocation capability," in Proc. 10th ACM conference on Computer and communications security, ser. CCS '03. New York, NY, USA: ACM, 2003, pp. 231–240. [Online]. Available: http://doi.acm.org/10.1145/948109.948141

[12] D. Hong and J.-S. Kang, "An efficient key distribution scheme with self-healing property," IEEE Commun. Lett., vol. 9, no. 8, pp. 759 – 761, aug 2005.