Protected Information Recovery for Decentralized detection in Wireless Sensor Networks

[1]T.N. RANGANADHAM, [2]N.PENCHALAIAH, [3] R.RANAPRATHAP

[1] CSE, AITS (Rajampet-Autonomous),Kadapa, India.

[2]CSE, AITS (Rajampet-Autonomous),Kadapa,India.

[3]CSE, AITS (Rajampet-Autonomous),Kadapa, India.

ABSTRACT:

Ciphertext-coverage attribute-founded security (CP-ABE) is a attractive cryptographic approach to the entry manipulate issues. Nonetheless, the situation of enforcing CP-ABE in decentralized DTNs supplies a number of security and alleviation difficulties with respect to the characteristic cancellation, key escrow, and synchronization of elements launched from unique regulators. We advocate two novel node replicated recognition approaches with special tradeoffs on process occasions and effectivity. The first one is depending on a allotted hash table (DHT), by which a absolutely decentralized, key-headquartered caching and verifying method is designed to capture duplicated nodes successfully. The method efficiency on mighty storage intake and high-quality safety level is hypothetically subtracted by means of a possibility design, and the causing equations, with essential enhancements for real utility, are bolstered by way of the units. Despite the fact that the DHT-founded system occurs upon identical interplay price as past strategies, it usually is regarded a little fine for some occasions. To handle this challenge, our 2nd allocated attention procedure, known as arbitrarily urged discovery, provides good interaction effectivity for heavy indicator programs, with the aid of a probabilistic recommended sending method along with unique preliminary route and boundary dedication.

***Keywords**: cipher text, DTN, DHT, efficiency*

1. INTRODUCTION:

Roy and Chuah offered storage nodes in DTNs the place information is stored or replicated such that most effective approved cellular nodes can access the vital know-how swiftly and efficiently. Many army functions require elevated safety of confidential data including entry control ways that are cryptographically enforced. In many circumstances, it is desirable to furnish differentiated entry services such that information access policies are defined over consumer attributes or roles, which are managed via the important thing authorities. For illustration, in a disruption-tolerant army network, a commander could store confidential expertise at a storage node, which should be accessed by means of individuals of “Battalion 1” who're collaborating in “vicinity 2.” on this case, it's a cheap assumption that a couple of key authorities are prone to control their possess dynamic attributes for infantrymen in their deployed areas or echelons, which would be more commonly transformed (e.G., the attribute representing current area of relocating soldiers). We check with this DTN structure where a couple of authorities limitation and control their possess attribute keys independently as a decentralized DTN.The thought of attribute-situated encryption (ABE) is a promising approach that fulfills the requisites for included information healing in DTNs.ABE features a procedure that permits an accessibility control over secured knowledge making use of accessibility instructions and attributed functions among individual important explanations and cipher textual content messages .Especially, cipher textual content-coverage ABE (CP-ABE) presents a scalable way of encrypting information such that the covered or defines the feature set that the decrypt or desires to acquire with the intention to decrypt the cipher written text. As a result, distinctive consumers are authorised to decrypt specific objects of knowledge per the safeguard plan. In this document, we reward two novel, sensible node replicated recognition approaches with one-of-a-kind tradeoffs on procedure circumstances and effectivity. The first present is relying on a allotted hash desk (DHT), through which a absolutely decentralized, key-headquartered caching and verifying approach is designed to capture duplicated nodes. The protocol’s effectivity on storage consumption and a primary security size are hypothetically subtracted through a possibility design, and the causing equations, with indispensable change for real application, are bolstered by means of the units .In compliance with our study, the extensive simulator outcome show that the DHT-centered method can identify node replicated with high safeguard stage and keeps powerful level of resistant to adversary’s strikes. Our second system, referred to as arbitrarily instructed discovery, is designed to provide extremely effective interplay performance with sufficient recognition possibility for heavy indicator methods. In the procedure, in the beginning nodes ship declaring know-how containing a neighbor-list along with a highest hop restrict to arbitrarily selected neighbors; then, the next idea transmission is managed by a probabilistic suggested method to roughly preserve a line property through the method as well as to have enough randomness for better effectivity on interaction and force against attacker .In addition, boundary dedication approach is employed to further slash interaction payload. For the duration of sending, developed nodes discover declaring know-how for node replicated recognition. By means of design, this method takes in practically little storage, and the units exhibit that it outperforms all other attention methods in the case of interaction fee, at the same time the consciousness likelihood is appropriate.

2. SCHEME CONSTRUCTION

In this subject, we offer a a couple of energy CP-ABE plan for included understanding restoration in decentralized DTNs. Each regional energy issues restrained custom-made and have key factors to a purchaser via executing included 2PC process with the fundamental energy. Every characteristic key of a consumer can be modified independently and immediately. For this reason, the scalability and protection may also be improved within the prompt plan. Because the first CP-ABE plan urged by way of Bethencourt et al., a multitude of CP-ABE strategies have been suggested. The next CP-ABE procedures are usually stimulated with the aid of extra extensive safety evidence within the traditional design. Nonetheless, many of the procedures didn't accomplish the expressiveness of the Bethencourt et al.'s plan, which described an efficient method that used to be colossal in that it accepted an comfortable or to show an accessibility predicate interms of any monotonic approach over facets. Hence, on this discipline, we create a change of the CP-ABE criteria partly depending on (but now not restrained to) Bethencourt et al.'s progress so they can make stronger the expressiveness of the accessibility control plan instead of making a new CP-ABE plan from the begining.

Let $\mathcal{T}$ be a tree representing an access structure. Each non leaf node of the tree represents a threshold gate.If $\mathrm{num}_x$is the number of children of a node xandKx is itsthreshold value, then $0 \leq Kx \leq numx$.Each foliage node x of the shrub is described by an feature and a limit value Kx=1 . Signifies the feature associated with the foliage node in the shrub. P(x) symbolizes the mother or father of the node in the shrub. The kids of every node are designated from 1 to num. The operate index(x) Profits such a variety associated with the node x. The catalog principles are exclusively allocated to nodes in the accessibility framework or a given key in an irrelavent way.Let $\mathcal{T}_x$ bethesubtreeof $\mathcal{T}$rooted at the node x .If as set ofattributes γsatisfies the accesstree $\mathcal{T}_x$,wedenoteitas $\mathcal{T}_x(\gamma) = 1$. We compute $\mathcal{T}_x(\gamma)$ recursivelyas follows. If x is a nonleaf node, evaluate $\mathcal{T}_{x'}(\gamma)$ for allChildrenof node x'. returns 1 iff at least $k_x$childrenreturn 1. Ifis a x leaf node, then $\mathcal{T}_x(\gamma)$returns 1 iff $\lambda_x \in \gamma$.Let $\mathbb{G}_0$ be a bilinear group of prime order andlet be agenerator of $\mathbb{G}_0$.Let $e : \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ denote the bilinearmap. A security parameter k,will determine the size of thegroups. We will also make use of Lagrange coefficients $\Delta_{i,\Lambda}$ forany $i \in \mathbb{Z}_p^*$ and a set, A ,ofelementsin $\mathbb{Z}_p^*$: define $\Delta_{i,\Lambda}(x) = \prod_{j \in \Lambda, j \neq i} \frac{x-j}{i-j}$. We will additionally employ a hash function $H : \{0,1\}^* \rightarrow \mathbb{G}_0$ to associate each attribute with a unique group factor in which we will design as a unique oracle.

In CP-ABE, purchaser key key factors involve a single customized key and a few feature most important reasons. The personalized key is exclusively recognized for each and every consumer to restrict collusion strike amongst purchasers with one-of-a-kind facets. The urged key construction procedure is which include the personal key production followed by way of the feature key creation ways. It uses mathematics blanketed 2PC procedure to remove the important thing escrow challenge such that not one of the regulators can check the entire key factors of consumers independently. In phrases of the computation rate, every local authority is required to perform two extra exponentiation operations. Each and every consumer needs to participate in multiplication operations for the important thing generation, which incurs negligible computation price in comparison with the other pairing or exponentiation operations. (The unique computation price will likely be analyzed in part V-C.) These expenses could be also incurred only for the initial key iteration procedures. Hence, the further computation overhead for the key iteration making use of the 2PC protocol is suitable in the system.

Data Encryption*:* When a sender wants to deliver its confidential Data M he defines the tree access structure T over the universe of attributes L, encrypts the data under to enforce attribute-based access control on the data, and stores it into the storage node.The encryption algorithm chooses a polynomial q_x for each Node X in the tree T These polynomials are chosen in a top down manner, starting from the root node R.For each node xin the tree T , the algorithmsets the degree d_x of the polynomial to be one less than the threshold value k_x ofthat node, that is, $d_x = k_x - 1$. For the root node R, it chooses aRandom $s \in \mathbb{Z}_p^*$ and sets $q_R(0) = s$. Then, it sets d_R other pointsof the polynomial q_R randomly to define it completely. Foranyother node xitsets $q_x(0) = q_{p(x)}(\mathrm{index}(x))$ and chooses d_x other points randomly to completely define q_x .Let Ybe the set of leaf nodes in the access tree. To encrypt amessage $M \in \mathbb{G}_1$ under the tree access structure T,itconstructsa After the construction of CT the emailer stores it to the storage space node safely. On receiving any data request question from a customer, the storage space node reacts with CT to the customer. It is worth noting that the emailer can define the access policy under features of any chosen set of multiple regulators without any limitations on the reasoning expressiveness in contrast to the previous multi power techniques.

Information Decryption*:* When a customer gets the ciphertext from the storage space node, the customer decrypts the ciphertext with its key key. The criteria works in a recursive way. We first define a recursive algorithm $\mathrm{DecryptNode}(\mathrm{CT}, \mathrm{SK}, x)$ That takes as inputs a ciphertext CT, , a private key SK, , which is associated with a set A of attributes, and a node x from the tree $\mathcal{T}$. It outputs a group element of $\mathbb{G}$ or $\perp$

Without loss of generality, we suppose that a user u_t performs the decryption algorithm. If x is a leaf node then define as follows . If $\lambda_x \in \Lambda$, then

Otherwise, we compute

$$\begin{aligned} F_x &= \prod_{z \in S_x} F_z^{\Delta_{i, S'_x}(0)}, \qquad \text{where} \quad \begin{array}{l} i = \mathrm{index}(z), \\ S'_x = \{\mathrm{index}(z) : z \in S_x\} \end{array} \\ &= \prod_{z \in S_x} (e(g, g)^{r_t \cdot q_z(0)})^{\Delta_{i, S'_x}(0)} \\ &= \prod_{z \in S_x} (e(g, g)^{r_t \cdot q_{p(z)}(\mathrm{index}(z))})^{\Delta_{i, S'_x}(0)} \\ &= \prod_{z \in S_x} e(g, g)^{r_t \cdot q_x(i) \cdot \Delta_{i, S'_x}(0)} \\ &= e(g, g)^{r_t \cdot q_x(0)} \qquad (2) \end{aligned}$$

and return the result.

We noticed that it is difficult to revoke specific feature important factors of a customer without rekeying the whole set of key elements of the customer in ABE key framework since the whole key set of a customer is limited with the same unique value to avoid any collusion strike. Therefore, revoking a individual feature in the program needs all customers who discuss the feature to upgrade all their key elements even if the other features of them are still legitimate. This seems very inefficient and may cause serious expense with regards to the calculations and interaction price, especially in large-scaled DTNs.For example, suppose that a useru_t is qualified with l differentattributes. Then, all l attribute keys of the user u_t are generatedwith the same random numberr_t in the ABE key architecture. When an attribute of the user is required to be revoked($l - 1$ other attribute keys of the user are still valid), the other valid $l - 1$ keys should be updated with another new r'_t that is different from r_t and delivered to the user. Unless the other$l - 1$ keys are updated, the attribute key that is to be revoked could be used as a valid key until their updates since it is still bound with the same r_t. Therefore, in order to revoke a singleattribute key of a user$O(l)$, keys of the user need to be updated. If n users are sharing the attribute, then total $O(nl)$ keys need to be updated in order to revoke just a single attribute in the system.

2.1 Key Update

When a customer comes to hold or fall an feature, the corresponding key should be modified to avoid the customer from obtaining the past or following secured information for in reverse or forward secrecy, respectively. The key upgrade process is released by delivering a be a part of or keep demand for some feature team from a user who wants to hold or fall the feature to the corresponding power. On invoice of the account modify demand for some feature categories, it notifies the space for storage node of the event. Without loss of generality, assume there is any account modify in G_i (e.g., a user comes to hold or drop an attribute λ_i at some time instance). Then, the update procedure progresses as follows.1)The storage node selects a random $s' \in \mathbb{Z}_p^*$ and a K'_{λ_i} which is different from the previous attribute group key K_λ Then, it re encrypts the ciphertextCT using the public parameters PK as

$$\begin{aligned}\mathrm{CT}' = \Big(\mathcal{T}, \tilde{C} = Me(g,g)^{(\alpha_1+\cdots+\alpha_m)(s+s')}, C = h^{s+s'}, \\ C_i = g^{q_i(0)+s'}, C'_i = \left(H(\lambda_i)^{q_i(0)+s'}\right)^{K'_{\lambda_i}}, \\ \forall y \in Y \setminus \{i\} : C_y = g^{q_y(0)+s'}, \\ C'_y = \left(H(\lambda_y)^{q_y(0)+s'}\right)^{K_{\lambda_y}}\Big).\end{aligned}$$

For the other feature categories that are not suffering from the account changes, the feature group important factors do not actually need to be modified.The storage node generates a new header messageHdr_i withK'_{λ_i} such that a set of attribute group members including a new joining user (for backward secrecy) or excluding a leaving user (for forward secrecy) can decrypt $K'_{\lambda_i} \cdot \forall y \in Y \setminus \{i\}, \mathsf{Hdr}$,remains the same.When a user sends a request query for the data afterward, thestorage node responds with the newly updated Hdr and ciphertext CT' encryptedunder the modified essential factors. It is worth noting that even if a customer is suspended from some feature categories, he may still be able to accessibility the information with the other features that he keeps provided that they fulfill the plan because they would still be efficient in the program.

3.DHT-BASED DETECTION PROTOCOL

The key of our first allocated awareness process is to create use of the DHT system to sort a decentralized caching and verifying software that can effectually identify duplicated nodes. Essentially, DHT allows indicator nodes to distributively advance an overlay program upon a exact indicator application and presents an efficient key-established redirecting inside the overlay program. A suggestion related to a key will likely be handed on through the overlay software to achieve a area node that is wholly identified by the important thing; the resource node does now not ought to specify or be aware of which node a message's area is—the DHT key-situated redirecting manages transport expertise via the message's key. Much more essential, understanding with a identical key shall be saved in a single region node. Those expertise construct the base for our first realization approach.As a beginning of a round of DHT-established replicated consciousness, the initiator indicates the recreation concept along with a unique seeds. Then, every viewer constructs a declaring suggestion for each next door neighbor node, which is most commonly known as an examinee of the viewer and the concept, and grants the inspiration with possibility personally. The discharge of the declaring likelihood is designed to diminish the interplay overwork in case of a excessive-node-measure system. Within the process, a message's DHT key that decides its redirecting and position is the hash price of concatenation of the seeds and the examinee identification. Through the DHT procedure, a declaring thought will gradually be handed on to a deterministic place node, so one can storage cache the identity-location couple and examine for node replicated recognition, performing as an examiner. Additionally, some advanced nodes additionally act as personnel to enhance force towards the attacker in an efficient means.

3.1 Distributed Hash Table

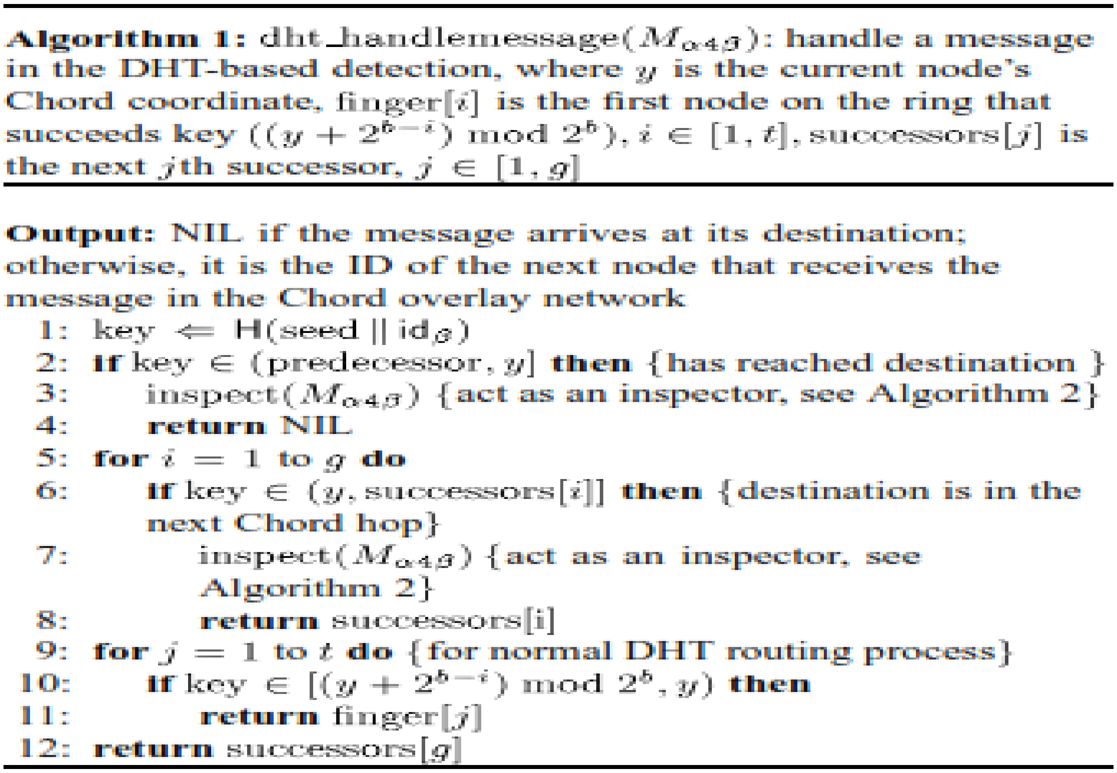
Earlier than snorkeling into the recognition procedure, we briefly current DHT approaches. In proposal, a allocated hash desk is a decentralized allotted process that supplies a key-established search service identical to a hash desk: (key, file) sets are saved within the DHT, and any taking part node can efficiently shop and get well information associated with specific fundamental explanations. By means of variety, DHT markets liability of maintaining the applying from main reasons to understanding amongst nodes in an efficient and healthy manner, which enables DHT to range to incredibly massive strategies and be appropriate to furnish as a provider of allocated node replicated attention. There are a couple of distinct types of DHT strategies, equivalent to CAN , be aware, and treat. Generally, CAN has least efficiency than others with regards to interaction fee and scalability, and it is hardly utilized in real tactics. Through comparison, notice is in most cases used, and we choose word as a DHT execution to show our process.

Nonetheless, our method can speedily transfer to boost upon treat and current same security and effectivity results.

3.2 Protocol Details: As a requirement, all nodes cooperatively build a Note overlay system over the indicator system. Duplicated node may not get involved in this process, but it does not give them any advantage of preventing recognition. The development of the overlay system is separate of node replicated recognition. 1) This node is the location node of the declaring concept.

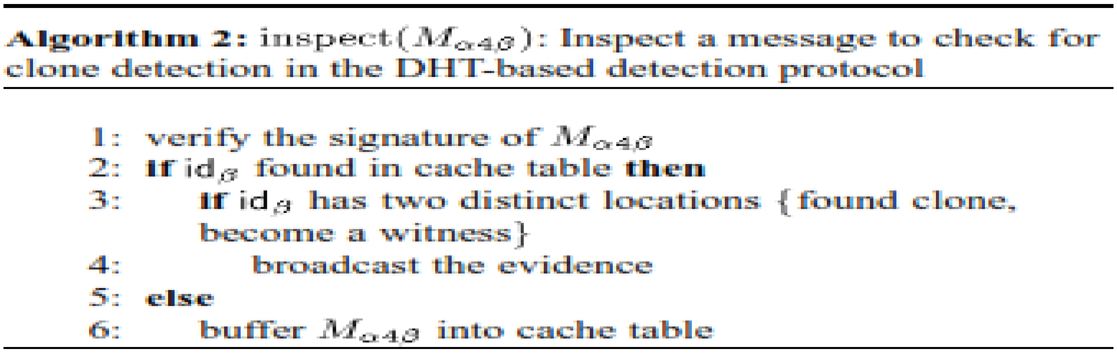
2) The location node is one of the successors of the node.

In other terms, the location node will be achieved in the next Note hop.



```
Algorithm 1: dht_handlemessage($M_{\alpha\to\beta}$): handle a message in the DHT-based detection, where $y$ is the current node's Chord coordinate, finger[$i$] is the first node on the ring that succeeds key $((y + 2^{b-i}) \bmod 2^b)$, $i \in [1, t]$, successors[$j$] is the next $j$th successor, $j \in [1, g]$

Output: NIL if the message arrives at its destination; otherwise, it is the ID of the next node that receives the message in the Chord overlay network
key ⇐ H(seed || id$_\beta$)
if key ∈ (predecessor, $y$] then {has reached destination }
    inspect($M_{\alpha\to\beta}$) {act as an inspector, see Algorithm 2}
    return NIL
for $i$ = 1 to $g$ do
    if key ∈ ($y$, successors[$i$]] then {destination is in the next Chord hop}
        inspect($M_{\alpha\to\beta}$) {act as an inspector, see Algorithm 2}
        return successors[i]
for $j$ = 1 to $t$ do {for normal DHT routing process}
    if key ∈ [$(y + 2^{b-i}) \bmod 2^b$, $y$) then
        return finger[$j$]
return successors[$g$]
```



```
Algorithm 2: inspect($M_{\alpha\to\beta}$): Inspect a message to check for clone detection in the DHT-based detection protocol

verify the signature of $M_{\alpha\to\beta}$
if id$_\beta$ found in cache table then
    if id$_\beta$ has two distinct locations {found clone, become a witness}
        broadcast the evidence
else
    buffer $M_{\alpha\to\beta}$ into cache table
```

4. SECURITY DISCUSSIONS

Validity of Detection:

The identification-established cryptographic system provides efficient identification verification and inspiration verification for the DHT-headquartered procedure. For this reason, the attacker cannot falsify duplicated nodes' IDs; neither can the change expertise finalized through reliability nodes. Moreover, a duplicated node cannot misinform its authorities about its place considering the fact that a made location could be some distance deviated from the interplay style of the authorities, which suffices to aware experts. Accordingly, the recognition ideas are amazing supplied gurus are sincere.As a result, nodes have details of their immediate forerunner and heir in the Not and. addition, each node .

Thwarting Framing Attack A become aware of cannot create an proof to structure reliability nodes considering that the proof step by step is which include declaring know-how from distinctive specialists, and any node can verify them. However, for any witness-based attention approach, akin to our two recommendations and approaches in Desk I, there's a precise chance that some unsafe professionals attempt to structure simple nodes through declaring fallacious places for them. To combat this strike, we gift a system that wants nodes to safeguard proof understanding they got and to maintain a charge desk for these gurus in proof. When a node is announced as a replicated in one or more facts, feel one in all its special locations is acknowledged by way of one of a kind specialists, then each and every of these authorities should be debited by way of . If a node's balance within the charge desk surpasses a limit, it should be suspended as good. We propose one for the limit. On this drawback, if a unsafe node tries to constitution an reliability node by means of declaring a flawed location for it, each nodes shall be suspended. This one-exchanging-one procedure is particularly affordable and efficient as we do not must differentiate which one is bad. When there is no framingattack in the network, integrity nodes are not often revoked on account that a clone node's situation may be acknowledged by means of many experts. At most, the form of suspended reliability nodes is not going to surpass the style of detrimental nodes**.**

Protecting Witnesses:

Officially, the hash points utilized in DHT do not have to be cryptographic hash aspects. In endeavor, cryptographic ones are ordinarily applied in the DHT procedures on the grounds that of their well always distinctive submission of outcome and keeping off prospective violations. For our approach, a cryptographic hash function is indeed needed seeing that it's going to limit the adversary's capabilities via program on as he cannot differentiate which nodes would extra possible be witnesses earlier than a circular of consciousness. After disclosure of the distinct seeds, dealing with Message-Discarding: The duplicated nodes may get rid of declaring knowledge by way of them. Our process is lengthy lasting against it due to the attribute of complete distributiveness and steadiness of the DHT-based system. If there are just a few duplicated nodes, the effect of this harmful endeavor will probably be in significant. When the style of duplicated nodes improves, more declaring understanding will assurance adequate form of witnesses. The items later certainly point out this effect.

5.SIMULATIONS FOR DHT-BASED PROTOCOL

We follow the DHT-based awareness system and run units to investigate efficiency broadly on the OMNeT++ structure. We variety the units in two approach circumstances. The first is an subjective approach following a distinctive chart variety. By way of definition, a detailed chart is a chart that's produced by means of establishing with a collection of vertices and including sides between them at distinct. The other one is a realistic unit-disk chart, in which nodes are always implemented in a rectangle and adhere to the traditional unit-disk bidirectional interaction sort. In our items, node interaction varies are dynamically modified such that the customary node level approximates d.

5.1 Performance on Varying Network Sizes

The following factors are used in the simulations: finger desk dimension t=16 successors desk dimension g=16, and node degreed=20. Two different principles of declaring possibility are used as 1.0 for pro-security and 0.2 for pro-communication price. We style and perform the first simulator to evaluate the protocol's efficiency on different system dimensions, which range from 500 to 5000. To be able to acquire relatively reasonable and similar outcomes, for each situation, 10 different system circumstances depending on the parameter configurations are designed. Each of those simulator accomplishments is estimated as a run; one run works 20 units of recognition. In each of those units, a unique seeds is produced, and two nodes are arbitrarily selected to set the same ID, that is, those two are duplicated nodes.

5.2 Results on Different Numbers of Cloned Nodes

We create the 2nd simulator to determine the protocol's effectivity on the one-of-a-kind form of duplicated nodes. We run items with one method dimension n=one hundred , and the duplicated node form improves from 2 to a hundred. We scan each and every situation with 10 operates, and for each and every run we do it again 200 units of node consciousness, in every of which a seeds is arbitrarily produced and nodes are arbitrarily chosen as imitations. Represents the simulator results concerning the normal dimension space for storage cache systems for reliability nodes and the fashioned style of witnesses, which help our protection justifications in field IV-C. In targeted, we are able to see that the approach exhibits robust force against message-discarding with the aid of duplicated nodes. Even if there are 10% nodes that maliciously eliminate expertise, the variety of witnesses is pretty excessive. In fact, the more duplicated nodes, the less the dimension space for storage cache systems for reliability nodes as space for storage consumption and the more witnesses as safeguard degree. For that reason, we particularly handiest ought to remember the border concern of for efficiency dimensions.

6. CONCLUSION

Indicator nodes lack tamper-resistant components and are subject to the node replicated strike. In this document, we present two allotted recognition protocols: One is depending on a allotted hash table, which types a note overlay approach and provides the key-founded redirecting, caching, and verifying elements for replicated consciousness, and the opposite uses probabilistic prompt technique to reap amazing interplay expense for suitable awareness likelihood. Even as the DHT-founded procedure supplies excessive security level for all kinds of sensor systems via one Deterministic discover and additional storage amazing, probabilistic witnesses, the arbitrarily advised discovery presents pleasant interplay n efficiency and little storage consumption for heavy sensor systems.

REFERENCES

[1] B. Parno, A. Perrig, and V. Gligor, “Distributed detection of node replication attacks in sensor networks,” in *Proc. IEEE Symp. Security Privacy*,2005, pp. 49–63.

[2] H. Balakrishnan, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica,“LookingupdatainP2Psystems,”*Commun. ACM*,vol.46,no.2,pp.43–48, 2003.

[3] Y. Zhang, W. Liu, W. Lou, and Y. Fang, “Location-based compromise tolerant security mechanisms for wireless sensor networks,” *IEEE J.Sel. Areas Commun.*, vol. 24, no. 2, pp. 247–260, Feb. 2006.

[4]S.Zhu,S.Setia,andS.Jajodia,“LEAP:Efficient security mechanismsfor large-scale distributed sensor networks,” in *Proc.10thACMCCS,*Washington, DC, 2003, pp. 62–72.

[5] R. Anderson, H. Chan, and A. Perrig, “Key infection: Smart trust forsmart dust,” in *Proc. 12th IEEE ICNP*, 2004, pp. 206–215.

[6] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, “A randomized,efficient, and distributed protocol for the detection of node replicationattacks in wireless sensor networks,” in *Proc. 8th ACM MobiHoc*, Montreal,QC, Canada, 2007, pp. 80–89.

[7] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, “Efficientdistributed detection of node replication attacks in sensor networks,”in *Proc.23rdACSAC*, 2007, pp. 257–267.

[8]H.Choi,S.Zhu,andT.F.LaPorta,“SET:Detectingnodeclonesinsensor networks,” in *Proc. 3rd SecureComm*, 2007, pp. 341–350.

[9] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, “On the detection of clones in sensor networks usingrandom key predistribution,” *IEEE Trans. Syst.s, Man, Cybern. C,Appl. Rev.*, vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[10] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributedsensor networks,” in *Proc. 9th ACM Conf. Comput. Commun.Security*, Washington, DC, 2002, pp. 41–47.

[11] A. Shamir, “Identity-based cryptosystems and signature schemes,” in *Proc. CRYPTO*, 1984, LNCS 196, pp. 47–53.

[12] R. Poovendran, C. Wang, and S. Roy, *Secure Localization and TimeSynchronization for Wireless Sensor and Ad Hoc Networks*.NewYork: Springer-Verlag, 2007.

[13] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Commun. Mag.*, vol. 40, no. 8, pp.102–114, Aug. 2002.

[14] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker,“A scalable content-addressable network,” in *Proc. SIGCOMM,*SanDiego, CA, 2001, pp. 161–172.