Multiple Server Based Sharing And Secured Data Management By Intrusion Detection System

Dr. Rekha Patil, Asmita Kadechur

Abstract— The user information has gained the higher interest as to communication has increased between the end users. The data manipulation has been the key aspect in the real time data exchange. The data increases exponentially hence the use of the storage location such as cloud or remote database has been developed. The storing and retrieving of the data has been challenged by the security threats. In this paper, for data transmission the use of the Routing protocol like AODV with the IDS technology and Slepian Wolf coding methods have been used for the data encoding and decoding. The dynamic multipath routing has been enabled to re-route in case of the attack. The system works under multiple scenario for the user need. In the attacking scenario, on detection of the honeypot node, the network is re-routed and repaired which results in achieving an optimal efficiency by adopting the Network Intrusion Detection System (NIDS) in the Trusted Network. The proposed concept of trace, repair or re-route has been a novel approach for secured and assured data manipulation in the cloud database.

Index Terms— Adhoc On Demand Distance Vector, Intrusion detection system, Honeypot node, Radcloud, Route Request, Route Reply, Slepian-Wolf Code.

———————————— ◆ ————————————

1 Introduction

The increased size of the data has given rise to the new concept of data exchange over the wireless systems. The transmission of the data can be viewed based on the criteria like

- Volume of the data
- Velocity which data generated shared and processed
- Variety- multi structure property which is due to type of multi user and data

The data processing tools feels difficult to manipulate as the data is being generated in multiple shorter cycles ranging from the hours to the milliseconds.

The concept of dividing the data D into the number of blocks N in such a way that the complete data can be re-constructed at the receiver end by using all the N blocks. Due to any attacker the N-1 block is missed or deleted or destroyed than the data cannot be completed and will be in unreadable format. By this method the key management technology in the digital cryptography can be implemented in dynamic way and will be reliable if in case of any misor-tunes occurs. The data will be secured by the unavailable of other data pieces[1]. A secret sharing data is non-perfect if some of the data subsets of the participants which cannot remove the value which has the partial information about the data. The ratio between the data secret sharing scheme is nothing but the ratio of maximum length of the data share and the secret key[3]. Oriol Farras, et.al [3] has dedicated his work to the search based on the ratio between the perfect and non-perfect secret sharing based schemes. Oriol Farras, et.al [3] has stated the data structure by the functional access the measures of the total amount of the data to be perfect and the non perfect by using the proposed concept.

In the system of wireless network data transmission where the end system of the users are always in the need of the data to be received in the encoded format, which has been transmitted or stored in some basic servers. The need of the data is high as it is used in the multiple scenarios of attacking and re-routing by routing protocols like AODV. Consider for an example ,the user of the client will ask for the data he or she needed which is supposed to be transmitted to them in a fixed route. The system should have the copy of the data in case of the data delivery fails and also it should be able to process mobile data to the user at multiple locations by using the trace, re- routing or repair of the path. Intruder or attackers present in the system will play an negative role in the real time data transmission between the need to end users. The data which has been transmitted from source to the destination has to be traversed between the nodes in the fixed route or path by using the specific routing protocol like AODV. The management of the data in the IDS assisted network by the encoding decoding scheme will be vital for data delivering in the cloud database. In the proposed work, for data transmission the use of the Routing protocol like AODV with the IDS technology and Slepian Wolf coding methods have been used for the data encoding and decoding. Jun Chen , et.al [6] explained the problem associated with the Slepian–Wolf coding in the dual channel coding issue . By the concept of the sense of sphere packing exponents and also the random coding exponents. The correct decoding exponents in the comparison of the two is a mirror-symmetrical. This mirror symmetry can be interpreted as the linear codebook-level duality in the concept of the Slepian–Wolf coding and also the dual channel coding. The conjunction of the coding exponent based values are synthesized by the expurgated exponents which will reveal the nonlinear term based the Slepian–Wolf codes which will be efficient compared to the linear type of the coding[6]. The main objective of the proposed work is to address the data security in the wireless network based data transmission over the cloud environment by using the re-routing algorithms. The user must be assured if the data delivery as it adopts the system in multiple scenario of attacking. The loopholes of the data transmission has to overcome by using the multilevel security checks. The main objective of the proposed work is to address the increasing popularity of the Cloud security issues in the data exchange environments. The security issues introduced through adaptation of the multiple network security by centralized IDS technology. Ability to visualize, control and inspect the network links and ports is required to ensure security.

2 INTRUSION DETECTION SYSTEM(IDS)

Intruder is a node or attacker or failure of link in the path of network where the data transmission has been assigned initially. These Intrusion detection and prevention system performs the security practices used in the blocking of the new threats in the data manipulation of the cloud or database management. The data which need to be traversed between the user and the receiver has to be capable of solving the data attacks.

The IDS system will perform the operation of resolving the issue in two ways:

- Pro-active IDS: Operation of IDS will takes place before attack based on the previous history of the network
- Reactive IDS: Operation will takes place after the attack happens based on the attack type and the place of attack.
- Hybrid IDS: This will be combines effect of both ids mentioned above. In our proposed work we are using the hybrid approach where the network is capable of resolving the attacker based on the history of the previous attack and also based on the new attack.

This is done through:

- Data file comparisons in the attacking nodes.
- Scanning processes finds the possible signs of honey pot nodes.
- Monitoring the network behavior to detect malicious intent.
- Monitoring the transmitted data status in the system database.

IDS can be broadly classified as

- Centralized IDS: where one node is implemented with the IDS and it does monitor all the network nodes. Less secured and less cost.
- Distributed IDS : in this all nodes are implemented with own IDS . Increases the overall security. But it increases the total cost of the system

  We have used the distributed IDS where we provide the high level of security and data security. The nodes(base station) has been implemented with the IDS in each nodes which will assure the data delivery the destination. The IDS will perform the data security by using the following operations based on the requirement:

  - Trace the honepot nodes

    It tracks the node where the failure of the data transmission has occurred. This may be due to the attacker or the link failure of the network. The process will seek the node of link which has failed and will update in the routing table of the path.
  - Repair the node

    After tracing the node which has caused the node to failure, the node will be repaired if it is possible. The simulator will perform this aspect based on the energy , distance or other constraints in real time environment.
  - Re-route by AODV

    If the honey pot node is non-repairable than the IDS will perform the dynamic rerouting by the AODV to reach the data to the destination cloud storage.

3 PROPOSED MODEL

The main objective of the proposed work is to address the data security in the wireless network based data transmission over the cloud environment by using the re-routing algorithms. The user must be assured if the data delivery as it adopts the system in multiple scenario of attacking. The loopholes of the data transmission has to overcome by using the multilevel security checks. The security issues introduced through adaptation of the multiple network security by centralized IDS technology. Ability to visualize, control and inspect the network links and ports is required to ensure security. We propose an IDS enhanced Slepian-Wolf coding based data transmission by AODV protocol for secured data transmission in the cloud database environment by using the concept of the data coded. The proposed method will achieve the optimal efficiency by adopting the IDS in case of the attacks. The proposed concept of trace, repair or re-route has been a novel approach for secured and assured data manipulation in the cloud database. The system works under multiple scenario for the user need. This achieves the optimal share size by the data coding. Performs trace, repair , reroute by AODV and is easy to manipulate under attacker by IDS.

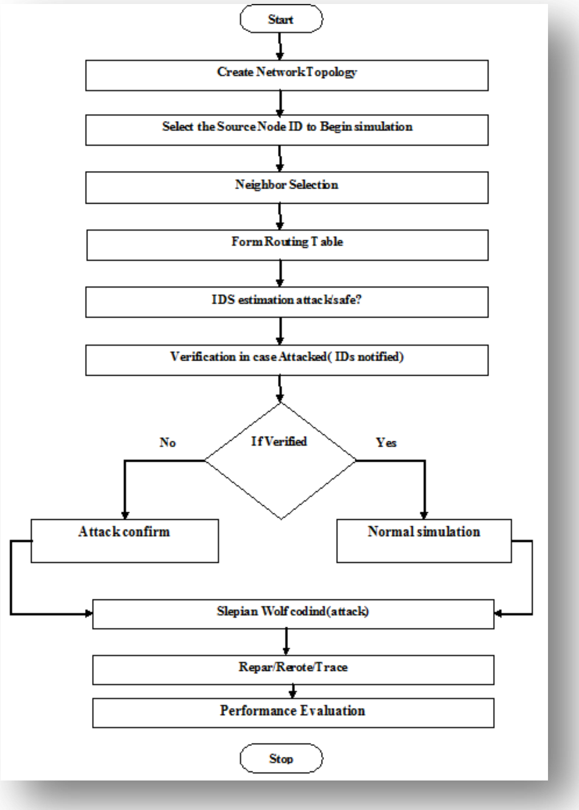


Fig 1.1. Flow chart of working of AODV and monitoring of IDS and Slepian Wolf code during normal and attacking scenario

The main modules can be listed as follows:

- Networks initialization (Network 1, Network 2)
- Physical File transmission over network (Router)
  1. Normal scenario
  2. Attacking scenario
- AODV based Routing
- IDS(Intruder detection System)
- Slepian-Wolf Coding
- Data storage in radcloud

- **NETWORK INITIALIZATION :**
  In this phase the (generally) network with the number of nodes, fixed path and multiple networks will be initialized. The source(Src) and the destination(Dst) are prefixed in the system. In the network each node is assumed to be sensor node having sense of data arrival and departure and is denoted by Si for the ith sensor node. The remaining set of nodes are denoted as v= {v1, v2, vN,}, |v |=N}, the communication links or edge E= {e1, e2, …, eN) neighbour.

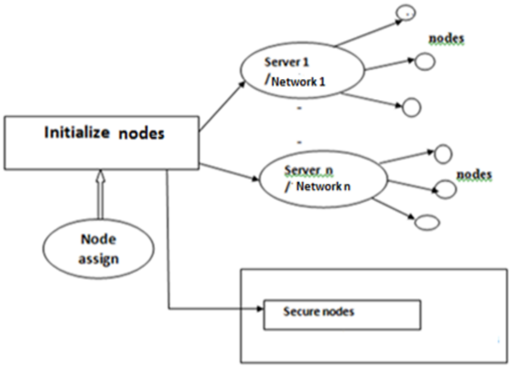


Fig 1.2. Network Initialization

In the figure 1.2, (generally) the network with the number of nodes, fixed path and multiple networks will be initialized

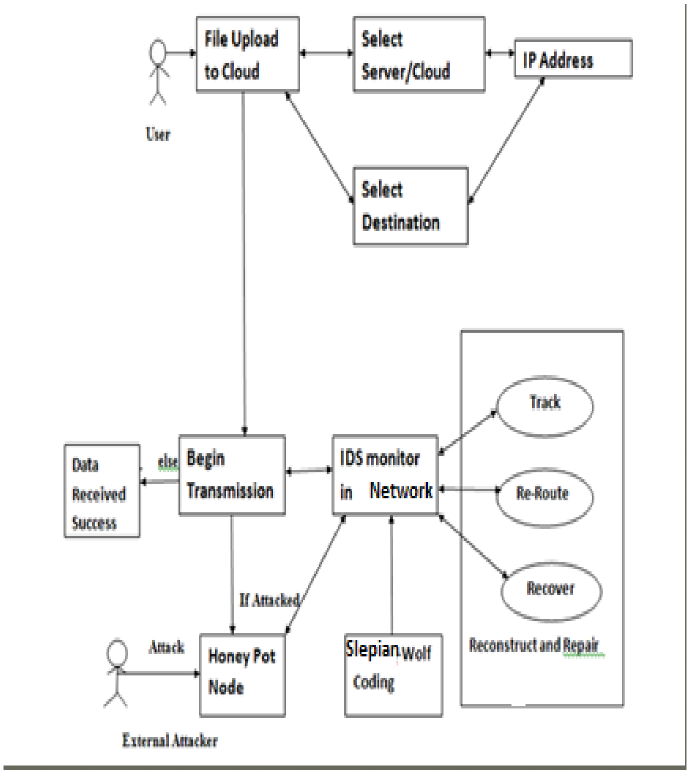
As we know that netwok consist of number of nodes hence the neighbor nodes in the network denoted as Vi= {i∈N|d (Vi, Vj) ≤D, n≠i},

Where, N – all nodes in network,
d (Vi, Vj) - distance between each node Vi, and Vj,
D – Travelling distance .

The cost for transmission of a k-bit packet or data over distance D is:
ETx (k, d) = k * Eelec + k * εfs * d2 d< d0 (1) = k * Eelec + k * εmp * d4 d>= d0
Where,
Eelec - base energy required to run the transmitter or receiver circuitry
εfs&εmp – Energy of the transmitter amplifier

To receive the message energy required is ERX (k) = k * Eelec

- **PHYSICAL FILE TRANSMISSION OVER NETWORK:**
  - Normal scenario
- In the figure 1.3, the transmission of the physical file has been achieved in the proposed work. The data file has been stored in the system storage initially which will be later saved in the online database. The data initially selected by the location based local server and used the Specific IP address of the receiver(IPV4 address).



- **Fig 1.3.** Physical File transmission over network

  Later the file is transmitted successfully through the prefixed path and the data is delivered to the receiver and stored in local device or the cloud database.

  - Attacking scenario
    During the file transmission the physical data is transferred through the fixed path. The attacker(honey pot node) will leak the data or link will be failed hence the IDS will be active. The tracing of failed node, repairing or re-routing is performed to secure the data delivery as shown in figure 1.3

AD HOC ON DEMAND DISTANCE VECTOR ROUTING (AODV)

In every route the nodes will be assigned the entry id. The AODV uses the unique Id of each nodes to achieve the goal.

The sequence number will be made available to the protocol during the built or routing table.
Nodes(N)={n1(id1),n2(id2)….n(idn)}

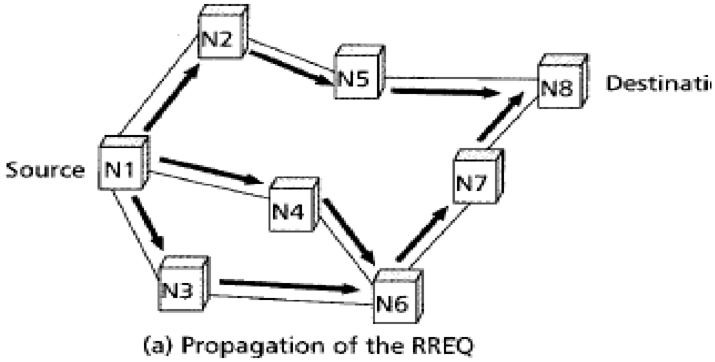
Before finalizing the route, the AODV performs the following sequence of message transmission operations like:

- Route Requests (RREQs)
- Route Replies (RREPs)
- Route Errors (RERRs)

The UDP will be receiving the messages known as sequence messages will be used to check the availability of the nodes. Request include the data type, data destination and the real time payload. The Request and the replies will be carried out in the sequence to confirm the node . If the node is available, than the route is selected and the operation is repeated till the destination if no errors found by the nodes. General networking scenario steps are as follows for the data transmission.

•Route-Request:

In this venture we presented one-sided back-off plot. Utilizing this plan we have send the R-REQ to the goal hub. To start with we need to ascertain the back-off delay. Source hub sends the R-REQ to their neighbor hubs and figures back-off defer utilizing this recipe, “tij = HopCount/∑kPikPkj”. τLettij indicate the back-off delay. Which hub has a shorter back-off postpone that hub select as a guide hub. This procedure will keep on reaching the goal hub as shown in fig 1.4. In the event that the goal hub might get the same R-REQ numerous circumstances, it will just answer to the principal R-REQ disregard others.

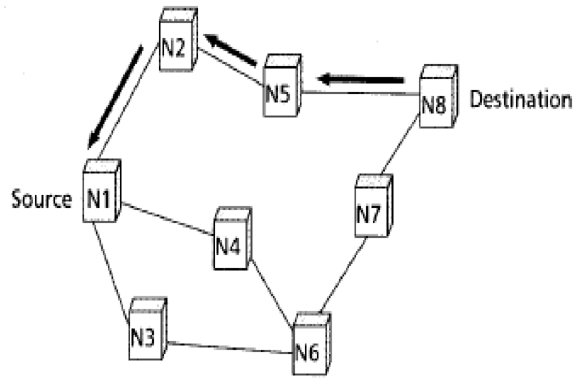


(a) Propagation of the RREQ

Fig 1.4. Propagation of the RREQ

•Route-Reply:

Subsequent to getting the R-REQ, the goal needs to send the R-REP to the source hub. In the fig 1.5, Before sending the R-REP the goal needs to check on the off chance that it is chosen jump hub. In the event that there is yes, it will send the R-REP else again look the chose bounce. Middle of the road hubs likewise check the hubs as a chose bounce hub. Assume that hub not a chose hub, the will be dropped generally forward the R-REP to source.



(b) Path of the RREP to the source

Fig1.5. Path of the RREP to the source

•Cooperative-Forwarding

The source hub communicates an information bundle, which incorporates the rundown of sending applicants and their needs. Those hopefuls take after the relegated needs to transfer the bundle. Every applicant, if got information bundle accurately, it will begin the back postponement. The A-CK send the source hub, which one of the applicant having shorter clock. On the off chance that no sending hopeful effectively got the information parcel, the sender will retransmit the information bundle if the retransmission component is empowered. A mid the information transmission if there is any impact happened, they will pick the partner hubs and send the information through the aide. Along these lines, the information will achieve the goal inside the specific time.

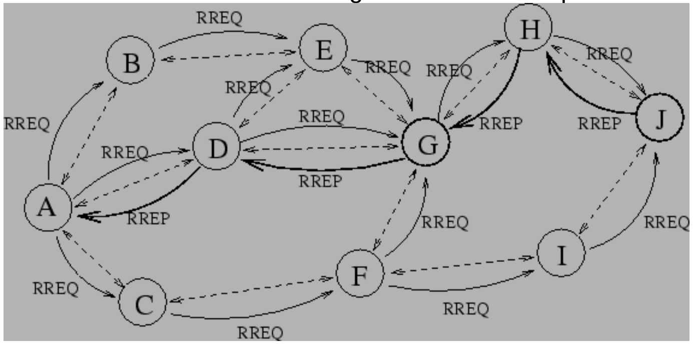


Fig1.6: Cooperative-Forwarding

AODV is a popular and well known routing protocol, it includes the route table management in it to avoid the looping and node failure. The route table will help to decide the path of the data to be transferred . the each node will be having information of the neighbor nodes with the help of the routing table.

The complete AODV algorithm can be expressed as follows:

- Destination nodes IP Address
- Destination nodes Sequence Number
- Valid flag
- Other state flags (e.g., available , unavailable, error)
- Network Interface protocol(UDP)
- Nodes Count
- Next Hop

- List of Precursors

3.1 AODV Algorithm:

```
1 The Source broadcast RREQ
2 Node received RREQ
3 If it is redundant RREQ, then Ignore or drop
4 If node is a gateway, then perform gateway mode procedure
5 If a local repair procedure is in progress, then en-queue the packets
6   If node is the destination, then
        Node create reverse route request(R-RREQ)
        Node generate R-RREQ
        Node sends R-RREQ
7   if it is not in the route table, then create an entry for the reverse route
8   if there is a fresher Seq_No or less hop_count, then update the route table
                else do not bother
9 If node is not the destination but it is a gateway, then forward the R-REQ
```

SLEPIAN WOLF CODING

The Slepian wolf coding is a distributed source coding based data coding methodology of two correlated sources. We have re-defined the SWC as needed to the proposed work.

If the sender send data to the end with its info data ‘d’ (‘1’ bits in d):

SWC.Encode(s,d) → (c,d):

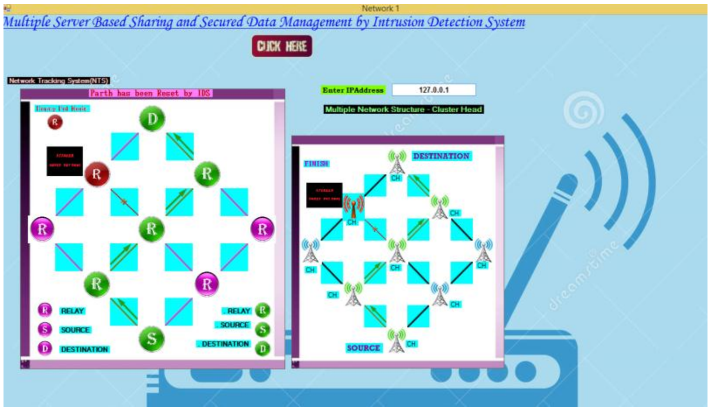
- Input : It is a binary string ‘s’ or data ‘d’
- Output : the coded block ‘c’ ,metadata ‘d’; numbering ‘1’ bits in s.
- Intake the data d : intake (transmit)
- Encode at Node N(Ed): each node trace the encode data as encoded
- Decode the data at the receiving end N(Dd): node trace the data
  By using the concept of sphere packing exponents and the random coding exponents. The correct decoding exponents in the comparison of the two is a mirror-symmetrical[6]. The conjunction of the coding exponent based values are synthesized by the expurgated exponents which will reveals the nonlinear term based the Slepian–Wolf codes which will be efficient compared to the linear type of the coding.

DATA STORAGE IN RADCLOUD:

The data which can be transmitted from the specific source and the destination has to be initially uploaded in the Radcloud, which is a free license cloud which will allow user to login and logout without major security concerns. The file will be uploaded to the cloud and later the file will be transmitted through the specified module. The cloud is independent of the protocol or algorithms used and hence can be executed directly also.

4 RESULT AND DISCUSSIONS

User uploads file to the RadCloud before transmission of a file from source to destination .The network1 also known as semitrusted network is monitored by Network Tracking System(NTS). The network2 also known as trusted network is monitored by Network Intrusion Detection System(NIDS). In the normal scenario, after entering systems IP address by the user, the path is selected and chosen file is sent from source to destination without any intruder attacking in this case. In the attacking scenario, initially the Network1 module wherein on file transmission, the NTS monitors the complete network and detects the honeypot node during transmission and re-routes the path and sends the file to destination as shown in fig 1.6.



Network 1

Multiple Server Based Sharing and Secured Data Management by Intrusion Detection System

Network Tracking System(NTS)

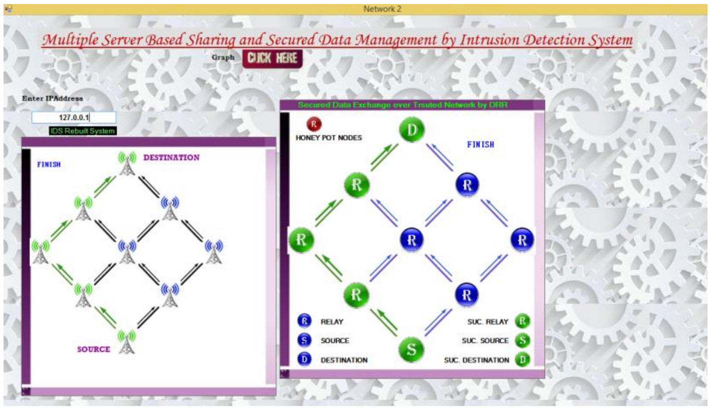
Parth has been Reset by IDS

Enter IPAddress 127.0.0.1

Multiple Network Structure - Cluster Head

Fig1.6. Network Tracking System(NTS) detects honeypot node and re-routes the path in Network 1

In the Network2, initially path or link initialization is done and NIDS monitors the path as shown in fig1.7



Network 2

Multiple Server Based Sharing and Secured Data Management by Intrusion Detection System

Enter IPAddress 127.0.0.1

IDS Rebuilt System

Secured Data Exchange over Trusted Network by DRR

Fig 1.7. Network intrusion detection system(NIDS) monitors Network 2 and repairs honeypot node and optimize the path.

After path initialization, NIDS detects honeypot node from predata of network1 and applies Slepian-Wolf Code by which it re-routes, repairs and also chooses best and shortest path to send the file to destination.

5 CONCLUSION

The process of providing the data security in the online data environment (cloud in general) has been in the high region of interest. The data need to be traversed from the source to destination through the intermediate nodes, these nodes has to be monitored by the proposed work of Slepian-Wolf coding based IDS system. The honeypot node or attacker has to be resolved, repaired or rerouted. The proposed work has been performed in the real and the attacking scenario which achieves the optimal share size by the data coding in the trusted network. The use of radcloud has assisted us in the real time data transmission through the nodes and data is received at the desired location.

REFERENCES

[1] A. Shamir, "How to share a secret", Communication of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

[2]B. Fortescue, and G. Gour, "Reducing the Quantum Communication Cost of Quantum Secret Sharing", IEEE Trans. Inf. Theory, no. 58, no. 10, pp. 6659-6666, 2012.

[3] O.Farras, T.Hansen, T.Kaced, and C.Padro ,"Optimal Non-perfect Uniform Secret Sharing Schemes",34thCryptologyConf.onAdvances in Cryptology (CRYPTO'14), pp. 217-234, 2014.

[4] J. Li, X. Chen, M. Li, J. Li, P.P.C. Lee, and W. Lou, "Secure Deduplication with Efficient and Reliable Convergent Key Management", IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 6, pp. 1615-1625, 2014.

[5] [13] L. Chunli, X. Jia, L. Tian, J. Jing, and M. Sun, "Efficient Ideal Threshold Secret Sharing Schemes Based on EXCLUSIVE-OR Operations", 4th Conf. on Network and System Security (NSS'10), pp. 136-143, 2010.

[6] J. Chen, D.K. He, A. Jagmohan, L.A.L. Montano, "On the linear codebook-level duality between Slepian-Wolf coding and channel coding", IEEE Trans. Inf. Theory, vol. 55, no. 12, pp. 5575-5590, 2009.

[7] E. Abbe, "Randomness and Dependencies Extraction via Polarization, With Applications to SlepianWolf Coding and Secrecy", IEEE Trans. Inf. Theory, vol. 61, no. 5, pp. 2388-2398, 2015.

[8] C. Cheng, J. Lee, T. Jiang, and T. Takagi, "Security Analysis and Improvements on Two Homomorphic Authentication Schemes for Network Coding", IEEE Trans. Inf. Forensics Security, vol. 11, no. 5, pp. 993-1002, 2016.

[9] C. Cheng, and T. Jiang, "An Efficient Homomorphic MAC with Small Key Size for Authenticationin Network Coding" ,IEEE Trans. Comput., vol. 62, no. 10, pp. 2096-2100, 2012.

[10] R. Johnson, D. Molnar, D. Song, and D. Wagner, "Homomorphic Signature Schemes", Cryptographer's Track at the RSA Conf. on Topics in Cryptology (CT-RSA), pp.244-262, 2002.

[11] C. Cheng, J. Lee, T. Jiang, and T. Takagi, "Security Analysis and Improvements on Two Homomorphic Authentication Schemes for Network Coding", IEEE Trans. Inf. Forensics Security, vol. 11, no. 5, pp. 993-1002, 2016.

[12] S. Gorbunov, V. Vaikuntanathan, and D. Wichs, "Leveled Fully Homomorphic Signatures from Standard Lattices", 47th ACM symposium on Theory of computing (STOC'15), pp. 469-477, 2015.

[13] D. Freeman, "Improved security for linearly homomorphic signatures: a generic framework", 15th conf. on Practice and Theory in Public Key Cryptography (PKC'12), pp. 697-714, 2012.

[14] B. Chen, R. Curtmola, G. Ateniese and R. Burns, "Remote Data Checking for Network Coding-based Distributed Storage Systems",2nd ACM Cloud Computing Sec .Workshop(CCSW'10),pp.31-42,2010