# Addressing Intra-Domain Network Security Issues through Secure Link-state Routing Protocol: A New Architectural Framework

Dijiang Huang[1#+], Qing Cao[2], Amit Sinha[1#], Marc J. Schniederjans[3], Cory Beard[1X], Lein Harn[1#], Deep Medhi[1#]

[1]Computer Science and Electrical Engineering Department, University of Missouri-Kansas City, Kansas City, MO 64110
[2]Henry W. Bloch School of Business and Public Administration, University of Missouri-Kansas City, MO 64110-2499
[3]College of Business Administration, University of Nebraska-Lincoln, Lincoln, NE 68588-0491
[+]Current affiliation: Computer Science & Engineering Department, Arizona State University, Tempe, AZ 85287-8809

Email: dijiang.huang@asu.edu, caoq@umkc.edu, amit.sinha@umkc.edu, mschniederjans1@unl.edu, beardc@umkc.edu, harnl@umkc.edu, dmedhi@umkc.edu

Final Revised April 2005

Keywords: Network Security; Link-State Protocol; Routing Authentication; Routing Confidentiality; Autonomous System/intra-domain routing

---

[#] Supported in part by a University of Missouri Research Board grant.
[X] Supported in part by NSF CAREER award grant # CNS-0133605.

The pervasive nature of information infrastructure coupled with threats for cyber terrorism makes network infrastructure security a critical area of interest for computer/network security practitioners and researchers. While there has been a significant amount of research on securing information content or software, securing network infrastructure has drawn attention sporadically over the years [1, 2, 5, 12]. One of the most critical infrastructure security issues involves securing routing infrastructure. Bellovin [1] in 1989 commented that *"Abuse of the routing mechanism and protocols is probably the simplest protocol-based attack available."* More recently, the following excerpts from the Computer Emergency Response Team – (CERT®) document [5] highlights the importance and imminent need for securing the routing infrastructure: *"One of the most recent and disturbing trends we have seen is an increase in intruder compromise and use of routers. … Reports indicate routers are being used by intruders as platforms for scanning activity. … Routers make attractive targets for intruders … routers are often less protected by security policy and monitoring technology … attacks based on direct attacks against the routing protocols that interconnect the networks comprising the Internet. We believe this to be an imminent and real threat with a potentially high impact."*

In order to understand routing infrastructure protection, we first start with a brief overview of the Internet routing infrastructure. For routing purpose, the infrastructure is divided into two domains: intra-domain and inter-domain. The entire routing infrastructure is a collection of intra-domain routing "regions" connected through an inter-domain functionality (see Figure 1). A particular intra-domain routing environment, also referred to as an Autonomous System (AS), is administered by a specific administrative authority; usually, this authority owns the routers in its domain, but not necessarily all the links that connect the intra-domain routers (since bandwidth is commonly leased from telecommunications carriers). Most commonly deployed routing protocols within an Autonomous System are Open Shortest Path First (OSPF) and Intermediate-System-to-Intermediate-System (IS-IS) routing protocols; they are both based on the concept of link-state routing (see SIDE-BAR). Neighboring Autonomous Systems exchange routing reachability information through an inter-domain functionality; in the Internet routing infrastructure, this functionality is accomplished through Border Gateway Protocol (BGP, currently, version-4). An intra-domain may be connected to multiple other intra-domains through inter-domain links and peering arrangement.

Routing attacks are attacks targeting routing protocols or attacks that rely on routers as weapons. A router is a network device that performs two main functions: it uses routing protocols to build up routing tables and secondly, it forwards data packets. The consequences of routing attacks can be noticeable and catastrophic as it can bring down a network infrastructure without causing any perceived physical damage to the network entities [7, 12]. In other words, since routers are network layer devices, faulty routers or routing protocols can cause malfunctions of the entire routing domain regardless of what services are running within the routing domain. Thus, routing attacks can have broad scale effects since these can deny or reduce communication capabilities of end systems. In this article, our scope is on categorizing various threats when link-state routing is employed in an intra-domain environment, followed by proposing preventative countermeasures to these threats, and finally to describe an architectural framework for

robustness of an intra-domain environment.

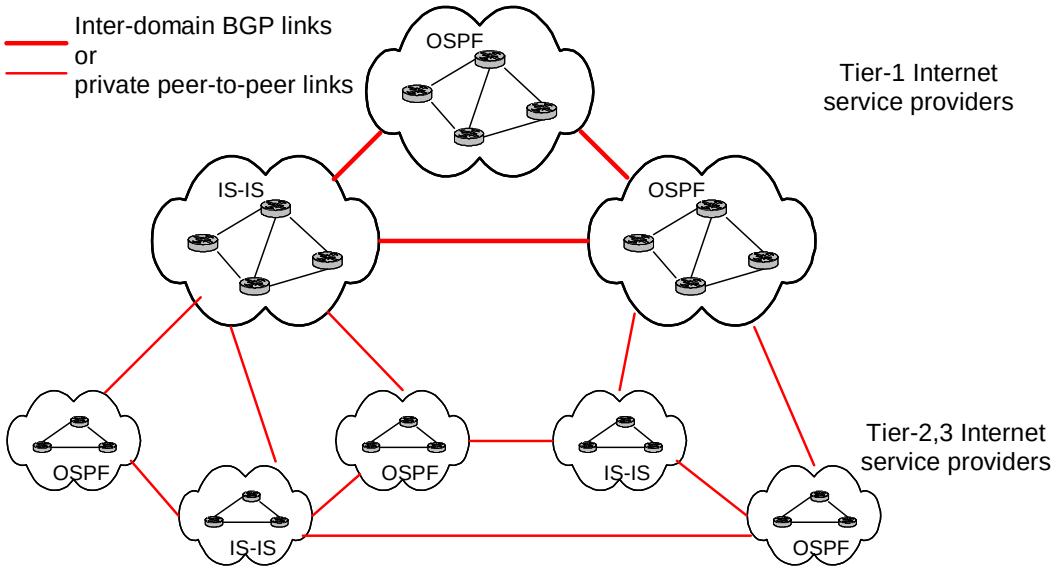


**Figure 1: Internet infrastructure connecting intra-domains through inter-domain links**

There are several reasons to consider the protection of an intra-domain routing infrastructure. If routers in a particular autonomous system (especially critical ones in the entire Internet routing infrastructure) are compromised, then it can affect transit traffic between different domains that are using this AS for reachability. If an autonomous system is decommissioned momentarily due to routing attacks, it can cause cascading effect on other Autonomous Systems through BGP, possibly leading to route flapping and delayed convergence and while such behavior has been identified earlier for routing CPU overload [9], it is similarly possible in the case of routing attacks. Another important consideration is that while routers in an intra-domain environment is owned by a particular administrative authority, they are "public" in the view of the Internet environment – that is, they are possible points of attacks much like end hosts or web servers connected to the Internet. Finally, since the links between routers in a geographically dispersed autonomous system are often leased, they are vulnerable to tapping by outsiders for information (including routing information exchange).

In link-state routing (see SIDE-BAR), a router receives LSAs from different routers; it may combine them into a link-state update (LSU) packet (see Figure 3) for flooding downstream. It is assumed that this router does not change the content of the LSAs received, but merely puts them together for forwarding purpose. For now, we assume that all routing information is generated in a clear-text format (discussion about how to protect it will be discussed later).

**Taxonomy of Network Routing Threats**

There are several sources of threat to a network routing infrastructure. In the context of routing infrastructure protection, it is immaterial what motivates these sources; what matters instead is whether these sources present a risk of security breaches to the infrastructure and to what level or extent. In an intra-domain routing infrastructure, there are legitimate users who have unlimited access to routers (for example, password-based access) and other legitimate users who have limited access; while clearly the former have more privilege than the latter, we classify both of them as 'insiders' in our taxonomy. In addition, there is another group of users who have external access to the infrastructure: 1) since routers in an intra-domain environment are still 'public' entities as far as the Internet is concerned, any users who are not legitimate users of the intra-domain infrastructure can conceivably try to "attack" such routers, much like the way web servers have been attacked for denial of service, 2) since a large geographically dispersed intra-domain environment consists of leased links (often, from telecommunications carriers), the possibility of a link being tapped for (and manipulation of) information cannot be completely ruled out. Thus, we can see that there is a second group of users (not legitimate users) who can do harm to an intra-domain routing infrastructure: we classify them as 'outsides' in our taxonomy.

| | Acquiring routing information (ARI) | Denial of service (DoS) | Routing-path manipulation (RPM) |
|---|---|---|---|
| Outsider | 1. Sniffing<br>2. Traffic analysis – Network tomography | 1. Interference<br>a. Add noise<br>b. Inject dummy routing/data traffic<br>c. Replay old packets | 1. Can manipulate |
| Insider | All capabilities of outsiders | All capabilities of outsiders | |
| | 1. Routing analysis<br>2. Deliberate exposure | 1. Interference<br>a. Not forwarding packets<br>b. Delay responses<br>c. Inject wrong routing packets<br>2. Overload<br>a. Overload CPU<br>b. Overload link-state database | 1. Impersonation<br>2. Falsification<br>a. Claim non-exist links<br>b. Misclaim exist links<br>c. Modify, insert, or substitute routing message |

**Table 1. Taxonomy of network routing attacks**.

It is important to recognize that an adversary can be either an insider or an

outsider; regardless, the primary goal of an adversary is to cause network routing to malfunction somehow. We base our classification by insiders and outsiders, rather then whether a user is being adversarial or not, since our classification allows us to consider goals and techniques of attacks more succinctly. We categorize threat possibilities for link-state routing into three types: acquiring routing information (ARI), denial of service (DoS), and routing-path manipulation (RPM). It may be noted that the first two are rather goals of an attacker (whether insider or outsider) while the third one is a technique to force routing and the network to malfunction—this technique is important to consider as a separate type due to the role of a link-state routing protocol in an intra-domain environment. In Table 1, we present our taxonomy of threats based on our user classification, and on identification of goals and techniques into three types. This is elaborated below.

*Threat possibilities from an outsider include:*

Acquiring routing information (ARI)

1. Sniffing: An outsider monitors and/or records routing exchanges between authorized routers to sniff for routing information; this cannot be ruled out, especially in a networking environment where links are leased.
2. Traffic analysis: An outsider gains routing information by analyzing the characteristics of the data traffic on a subverted link. Network tomography is a technique that can be attackers to derive network topology and network traffic allocation pattern by measuring end-to-end performance of the network (such as counts of sent/received packets, time delays between sent/received packets, etc.).

Denial of Service (DoS)

1. Interference: An outsider blocks routing exchanges between authorized routers to disrupt routing operations. The outsider can add noises to prevent the legitimate routers from receiving the routing information correctly, inject dummy data or routing packets to saturate the communication link, or replay old routing packets to cause the routing to malfunction.

Routing-path manipulation (RPM)

1. An outsider can manipulate the routing paths by disseminating forged routing information.

*Threat possibilities from an insider include:*

Compared to an outsider, an insider not only possesses all the capabilities of an outsider but also has the following additional capabilities.

Acquiring routing information (ARI)

1. Routing analysis: The routing information (i.e., LSA) is flooded within the link-state routing domain. All routers maintain the same network topology. As such, it

is easier for an insider to derive network topology, network routing and network resource allocation patterns (bandwidth of each link or traffic load on links).
2. Deliberate exposure: An insider intentionally releases routing information to others, such as outsiders or those who are not authorized to receive the exposed information.

Denial of Service (DoS)

1. Interference: Since an insider is a legitimate participant who has control over network routers, it can take actions to drop received routing packets (LSUs/LSAs), delay the responses of the received routing packets (which can prolong the routing convergence time and cause instability of the system), or inject wrong routing information to prevent other routers from building correct routing tables.
2. Overload: An insider can place excess burden on legitimate routers. For example, the insider can create an excessive amount of link-state packets that other routers within the network are not able to handle. In addition, the insider can overload the routing database to prevent other routers from building up the routing table.

Routing-path manipulation (RPM)

1. Impersonation: this refers to an insider claiming to be another legitimate "router" and performs routing functions. Impersonation enables the insider to successfully carry out other threats (such as falsification) causing additional threat consequences. For example, by impersonating a legitimate router, the insider can successfully convince a receiver to accept forged routing packets if all routers use the same shared key to verify the routing packets. In this way, the insider can create a shorter path to attract data traffic or create a longer path to expel data traffic. Thus, the insider can manipulate the routing paths more efficiently by impersonating multiple routers rather than changing its own link weights.
2. Falsification: A router held hostage by an insider can send false routing information. It can also send non-existing or wrong LSAs of itself. The insider can also alter/drop the forwarded LSAs originated from other routers. By impersonating a legitimate router, the insider can forge LSAs for non-existent/existing communication links in any part of the link-state routing domain. Another goal of the insider is to create shorter or longer paths between communication peers, and thus deviates the data traffic to a host controller by the attacker.

In summary, network routing security rests on confidentiality, integrity, and availability. These three aspects are closely related to threat possibilities that we have discussed thus far: acquiring routing information (ARI), denial of service (DoS), and routing-path manipulation (RPM), respectively. That is, ARI is related to confidentiality of a router, DoS related to the availability of a router, and RPM primarily relates to the integrity of a router.

**Link-state Routing Security Mechanisms**

The challenges imposed by the enormity and diversity of network routing threats

for an intra-domain routing environment have prompted the need to develop a variety of preventive techniques. In order to properly discuss how to prevent or minimize attacks, we first discuss preventive cryptographic countermeasures. It may be noted that preventive cryptographic countermeasures, by themselves, can do little to prevent DoS attacks. Most of the current solutions to DoS attacks are reactive solutions, i.e., solutions that depend on intrusion detection systems (IDS), which is beyond the scope of this research. However, we will discuss later how to create multiple trusted routing domains to mitigate the consequence of DoS attacks.

*Preventive cryptographic countermeasures:*

It may be noted that the confidentiality ensures that no unauthorized entities can decipher the routing information on its way to a destination. Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication). The interpretations of integrity and authentication vary, as do the contexts in which they arise. In the context/setting of a link-state routing environment, authentication is generally considered as both data integrity and origin integrity.

First, we briefly summarize work by other researchers. In recent link-state routing protocol standards, RFC 2328 [10] for OSPFv2 (OSPF version-2), packet level authentication capability is now available. Note that this refers to a routing packet such as a link-state update (LSU) packet which usually contains multiple LSAs; that is, the authentication is provided only at the LSU level, not at the LSA level. By using a keyed cryptographic hash (i.e., a message authentication code), a shared secret key is configured in all routers attached to a common network/subnet and each LSU is authenticated. An example of authentication techniques is keyed hashing for message authentication (HMAC). We note that the operation of HMAC also provides data integrity checking; only authorized users (possessor of a shared key) can generate and verify HMAC. Similarly, digital signature for OSPF (See RFC 2154 [11]) also provides both data integrity and origin integrity. In this work, we consider authentication as providing both data integrity and origin integrity.

Our approach focuses on the following two preventive cryptographic countermeasures: confidentiality and authentication. These two countermeasures can provide protection at either the *packet level* (PL) or the *information level* (IL), shown in Figure 3. If we assume a routing packet to be a bus filled with a group of passengers, PL and IL represent the cryptographic countermeasures being provided for the bus and each individual passenger, respectively. Besides authentication and confidentiality, there are two other important concepts we need to introduce; they are *point-to-point* (P2P) and *end-to-end* (E2E). In terms of authentication, P2P means that the generation and verification of an authentication code are performed by every forwarding router; while E2E means that the generation of an authentication code is performed only at the originating router, all the forwarding routers and termination routers are part of the end system, and they only perform verification. In Table 2, we summarize two main preventive cryptographic countermeasures needed for link-state routing protocols; the table also includes labeling currently available approaches.

| Methods | Level | Label | Description | Examples |
|---|---|---|---|---|
| Authentication | Packet Level | $PLA_{P2P}$ | Packet level, point-to-point authentication | OSPFv2 ([10]) and OSPFv3 ([4]) |
| | | $PLA_{E2E}$ | Packet level, end-to-end authentication | N/A |
| | Information Level | $ILA_{P2P}$ | Information level, point-to-point authentication | N/A |
| | | $ILA_{E2E}$ | Information level, end-to-end authentication | OSPF with digital signature ([11]) |
| Confidentiality | Packet Level | $C_{PL}$ | Confidentiality for the whole packet | OSPFv3 ([4]) |
| | Information Level | $C_{IL}$ | Confidentiality for the information within the packet | N/A |

**Table 2. Preventive cryptographic countermeasures.**

As one can see, only some of cryptographic countermeasures presented in Table 2 have been addressed in the existing literature, namely, $PLA_{P2P}$ and $ILA_{E2E}$. Researchers in our team (see Huang, Sinha and Medhi [6, 7] for details) have addressed additional measures such as the *double authentication* (DA) scheme to set up an authentication chain from the source to destination. In this scheme, each router generates two authentication codes for the LSA: one is used for verification by all its neighbors; the other is used for verification by all routers except its neighbors (see SIDE-BAR for a discussion of the DA scheme). Generally speaking, digital signatures use asymmetric (public / private key) encryption algorithm and digital signatures operate roughly 100 to 1000 times slower (depend on which cryptographic algorithm is used) than symmetric encryption algorithms, such as HMAC, under same hardware constraints. The DA scheme (basically lies between $ILA_{E2E}$ and $ILA_{P2P}$) is aimed to provide similar security features of digital signatures, and at the same time, it has less computational overhead as compared to using a digital signature scheme. Note that $ILA_{P2P}$ does not provide protection from insider attacks, moreover, it involves more computational overhead than $PLA_{P2P}$ schemes. To date, no $ILA_{P2P}$ authentication schemes have been proposed. Regardless, based on the above analysis, using both $PLA_{P2P}$ and $ILA_{E2E}$, it is possible to design a secure intra-domain routing environment which can provide strong cryptographic countermeasures to prevent insider attacks (such as impersonation and falsification by claiming/misclaiming other routers' links and modifying/inserting/substituting the forwarded LSAs).

To date, there has been no $C_{IL}$ proposed for link-state routing. Our proposed approach is to use $C_{IL}$ and $ILA_{E2E}$ for link-state routing as the foundation to build a new secure link-state routing framework for intra-domain routing. To deploy $C_{IL}$, routing information is categorized by multiple groups. By carefully assigning group keys to routers, we can partition network resource into multiple routing domains. For example, consider a router with several outgoing links; it can encrypt LSAs for some links using one key and encrypt LSAs for other links using another key. Thus, only routers that have the correct key can decrypt the routing information. This strategy can also be applied to a

single link, i.e., a router can partition the bandwidth of a link into multiple portions and create/encrypt an LSA for each portion. This approach has several benefits:

- It prevents outsiders' sniffing attacks (we assume that the crypto key length is long enough to prevent brutal force attack within a maintenance cycle – periodically update the crypto keys).
- It mitigates outsiders' traffic-analysis attack: Since link-states are encrypted and a router may or may not possess the decrypting key, routers can maintain different network topology and shortest path tree. Thus, the data flow may not follow the same shortest path, which can prevent attackers from deriving correct network topology or traffic allocation pattern.
- An insider has limited information of the network, which can mitigate routing analysis and deliberate exposure attacks.

To implement $C_{IL}$, an efficient secure group key management scheme, which supports many-to-many secure group communication, is needed. Many-to-many secure group communication requires that each group member (router in our case) with a group population of size $n$ can communicate with any subgroup of members securely; this means a group member would need to possess $2^{n-1}$-1 keys. When $n$ is large, it is not possible for a group member to store $2^{n-1}$-1 number of keys. To solve this problem, a centralized key server can be in charge of the group key management functionality. However, the centralized key server is vulnerable to single point failure. In addition, long key setup delay and communication overhead due to key setup prevent the centralized scheme from being used for secure many-to-many group communication needed between a subgroup of routers. To solve the above discussed problems, Huang and Medhi (2004) [8] have proposed a novel key-chain based many-to-many secure group communication scheme and a key agreement protocol. The proposed group Key Management (KM) scheme involves two phases: the key predistribution phase and the group communication phase. During the key predistribution phase, a set of secrets is preinstalled in each group member (a router) via offline methods, such as manual installation or online dedicate secure channels. In order to construct the secure group keying scheme, this scheme utilizes the linear hierarchical structure of one-way function chain (such as hash chain). A unique value from each one-way function chain is distributed (however, multiple one-way function chains need to be constructed in advance). Based on the predistributed one-way function values (also called secrets) and the linear derivative relations of one-way function chains, each group member can self-derive any desired subgroup key. Thus, during the group communication phase, each group member (router) can self-generate any possible subgroup key at anytime *without* depending on a trusted third party (such as KM) or negotiating first among group members for any verification; that is, communication overhead due to such set-up can be avoided. Note that a subgroup key is a shared key that is known only to the corresponding subgroup members.

*Other Security Supporting Mechanisms*

To build a highly secure routing system, several supporting mechanisms are also needed. For example, DoS attacks are difficult to prevent. The most efficient countering technique is to identify the DoS attack and respond to it quickly. An IDS (intrusion detection system) is a system that collects information from a variety of systems and

network sources, and then analyzes the information for signs of intrusion and misuse. Chang et al. [3] proposed a real-time IDS for link-state routing protocols. This IDS is based on *simple network management protocol* (SNMPv3), which can be used to collect system status and intrusion alerts from the network. To respond to attacks, we need a network resource management system to manage routers, such as isolating subverted routers, changing link weights, informing a key management system to redistribute keys, and so on. This will be addressed in the next section.

**An Architectural Framework for Secure Link-state Routing**

Now that we have covered various components and proposed approaches, we are ready to present our entire secure routing architectural framework which is based on security techniques (authentication and confidentiality) for the link-state routing protocol. In our proposed routing framework shown in Figure 2, there are five components: trust routing domains (TRDs), network resource management (NRM), key management (KM), traffic management (TM), and intrusion Detection System (IDS). Arrows within Figure 2 represent the communication relations among different components.

The entire routing domain can be divided into multiple routing sub-domains. We refer to such a sub-domain as a TRD. The framework may not need/imply the division of the administrative domain into TRDs. Every router that belongs to a particular TRD will have complete routing information of its own TRD, but not others. We use the cryptographic techniques $ILA_{E2E}$ and $C_{IL}$ to build the TRD framework. We also assume each router has the capability of link bandwidth control. For example, the bandwidth of a communication link of each router would need to be divided by using different encryption/decryption/authentication keys. While bandwidth partitioning is not directly available in today's routers, this can be accomplished through the concept of multiple virtual links due to availability of virtual link concept in the current generation of routers; nevertheless, the actual bandwidth control mechanism would need to be a new functionality. Thus, a subset of network resources, which is composed by multiple network links by using the same encryption/decryption/authentication key, will build a TRD.

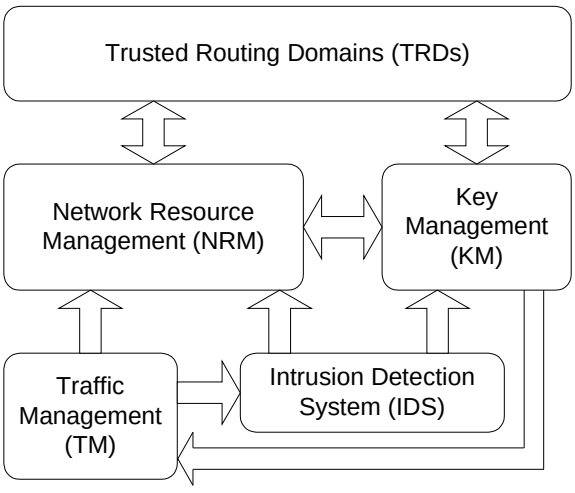


**Figure 2. Secure framework for link state routing.**

The network resource management (NRM) plays an important role in our framework to provide survivability. It serves as a coordinating center to create or withdraw a TRD. The traffic management (TM) reports the network resources allocation information to NRM and intrusion detection system (IDS) reports the network security events to NRM. Based on the reported information, NRM makes the decision on creating or withdrawing a particular TRD.

An efficient key management (KM) needs an efficient keying scheme that can reduce the management overhead such as key setup delay and communication overhead due to key setup. Creating TRDs in a routing domain and providing $ILA_{E2E}$ and $C_{IL}$ to the routing information require an efficient symmetric keying scheme. The keying scheme would be deemed suitable for this purpose if it displays the following features:

- Shared key scheme is preferred in order to minimize computational overhead.
- Each TRD is formed by using the same shared key and this shared key is only shared among those TRD members (a subgroup of routers). KM needs to be flexible in order to support group/subgroup communication to reduce overhead caused by subgroup formation processes. The secure many-to-many group communication scheme presented in [8] (and briefly described earlier) is such a candidate for KM.

To build TRDs, the proposed framework ensures the independence among all TRDs that provide a degree of survivability when a router is compromised. That is, any single router failure of a TRD would not affect other TRDs.

*Framework Evaluation:*

We have conducted an initial evaluation of the robustness of the proposed framework. The evaluation results show the following benefits:

- Proposed framework mitigates the effect of network tomography. It can mitigate the DoS attacks caused by both outsiders and insiders; it can mitigate the routing analysis and deliberate exposure attacks by insiders; and finally its use of $ILA_{P2P}$ provides integrity and origin authentication to prevent insiders from impersonating and forging routing information of other legitimate routers.
- Proposed security features are adds-on components and hence do not change operational functionalities of current link-state routing protocols. For example, security extensions can be implemented using opaque option in OSPF protocol.
- The router CPU usage is usually dominated by the length of time it takes to run the shortest path calculation. Our comparison study shows that the adds-on processing overhead for processing link-state advertisements is minimal to shortest path calculation; furthermore, LSA processing is done at a different time than shortest path calculations.
- Routers have the ability to handle the extra processing required for the proposed framework, with some increase in memory requirement.

We are currently doing further work on understanding best ways to accomplish division of TRDs, overall network performance issues and more detailed robustness analysis of the overall architecture.

**Summary**

Network survivability has been studied extensively from the view of node and link failures. The domain of survivability goes beyond just the physical failures and one

needs to address this issue when faced with security threats that can render the network logically dysfunctional without causing any physical damage. An intra-domain routing environment may encounter several security threats that can eventually make network routing susceptible to a number of attacks. We discuss potential attacks and propose a new secure routing framework based on security techniques (authentication and confidentiality) for a link-state routing protocol, applicable in an intra-domain routing environment. The proposed framework emphasizes the use of efficient cryptographic countermeasures for network survivability against security threats to link-state routing protocols. The framework relies on providing information level authentication and information level confidentiality that can be imbedded in link-state routing protocols with assistance of a key management system which uses secure group communication. Our proposed secure network routing framework is a major step towards providing security professionals with an effective platform as deterrence to network attacks. It will be worthwhile to look into the balance between network security/performance and cost issues (i.e., cost of routers and routing protocols) in practices; furthermore, it will also be important to see the results of the implementation of the proposed framework. We leave these issues to be addressed in future research.

**References**


1. Bellovin, S.M., Security problems in the TCP/IP protocol suite, *Computer Communication Review* 19, 2 (1989), 32-48.
2. Chakrabarti, A., and Manimaran, G., Internet infrastructure security: A taxonomy. *IEEE Network* 16, 6 (Nov. 2002), 13-21.
3. Chang, H.Y., Wu, S.F., and Jou, Y.F., Real-time protocol analysis for detecting link-state routing protocol attacks. *ACM Transaction on Information and System Security* 4, (Feb. 2001), 1-36.
4. Gupta, M., and Melam, N.S. Authentication/Confidentiality for OSPFv3, *IETF Internet draft*, (Dec. 2004).
5. Houle, K. J., Weaver, G. M., Long, N, and Thomas, R. Trends in denial of service attack technology, *CERT® Coordination Center document*, 2001.
6. Huang, D., Sinha, A., and Medhi, D. A double authentication scheme to detect impersonation attack in link-state routing protocols, in *Proceedings of IEEE International Conference on Communications* (May 2003), 1723-1727.
7. Huang, D., Sinha, A., and D. Medhi, A key distribution scheme for double authentication in link-state routing protocol, in *Proceedings of 24th IEEE International Performance Computing and Communications Conference* (Apr. 2005).
8. Huang, D. and Medhi, D., A Key-chain based keying scheme for many-to-many secure group communication. *ACM Transactions on Information and System Security* 7, 4, (Nov. 2004), 523-552.
9. Labovitz, C., Malan, G. R., and Jahanian, F., Internet routing instability. *IEEE/ACM Transactions on Networking* 6 (1998), 515–528.
10. Moy, J. OSPF Version 2, *IETF RFC 2328*, (Apr. 1998).
11. Murphy, S., Badger, M., and Wellington, B. OSPF with Digital Signatures, IETF *RFC 2154*, (Jun 1997).
12. Papadimitratos, P., and Haas, Z.J. Securing the internet routing infrastructure. *IEEE Communications* 40, 10 (Oct. 2002), 60-68.

**SIDE-BAR on Link-State Routing**

A router sends information about its outgoing links ("link-states") to all its neighboring routers either periodically or when an event (for example, a failure) triggers such an advertisement; this advertisement is called link-state advertisement, LSA in short. A typical LSA contains link metrics which may be based on information such as hop count, bandwidth, delay, and so on; furthermore, an LSA for a link can contain multiple link metrics. Upon receiving an LSA from its neighbor, a router is required to make certain decisions: if this router has already received the same LSA (via another router), it will drop it; otherwise, this router will forward the LSA to all its neighbors except to the sending router. Thus, the forwarding takes place in a point-to-point basis, this forwarding procedure is called *flooding* and it continues until every router in the network receives the most recent LSA. In order to allow a receiving router to determine if it has the most recent LSA for a particular link, each LSA is stamped with a sequence number before it is disseminated by the originating router; if a router needs to generate a new LSA for any of its outgoing links, it increments the sequence number and starts the new advertisement that includes the newly stamped sequence number. Upon receiving LSAs of different links, each router builds a link-state database that also serves as topological information; using the metric contained in the LSA, each router can compute shortest path routing to all destination routers in its domain using Dijkstra's algorithm, and builds a packet forwarding table ("next-hop"). This forwarding table is used in determining how to handle an incoming data packet which is not meant for itself.

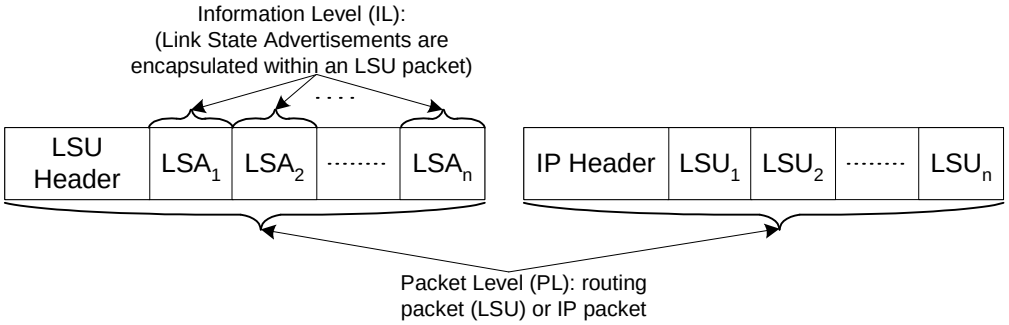


**Figure 3: Routing information encapsulation and illustrations of Packet Level (PL) and Information Level (IL)**

**SIDE-BAR on the Double Authentication Scheme**

The double authentication (DA) scheme presented in [6, 7] is designed to prevent impersonation attacks. In the DA scheme, the flooded LSAs are individually authenticated twice by two different keys, i.e., each LSA is signed twice by every router when it floods the LSA to its neighbor(s). Authentication codes are then appended to each individual LSA. Shown in Figure 1, node *i* originates an LSA. It then generates two authentication codes $A_{ik}$ and $A_{ij}$ by using shared key between pairs (*i*,*k*) and (*i*,*j*), respectively. After a neighbor node *j* receives the LSA, it authenticates the LSA based on the second code $A_{ij}$. Once the authentication is passed, node j generates two new authentication codes $A_{jl}$ and $A_{jk}$ by using shared key between pairs (*j*,*l*) and (*j*,*k*). Note that the authentication code $A_{ik}$ is also attached with the forwarded LSA and $A_{ik}$ can be used to verify that node *j* does not compromise the LSA. The presented forwarding and authenticating procedures will continue until all nodes in the network receive the LSA. Choosing DA scheme over other authentication schemes, such as packet-level (such as specified in RFC 2328) and information level (such as specified in RFC 2154), is the trade-offs between the consideration of security strength and computation overhead. DA scheme provides stronger authentication than packet-level authentication scheme but less computation overhead than information-level authentication scheme.

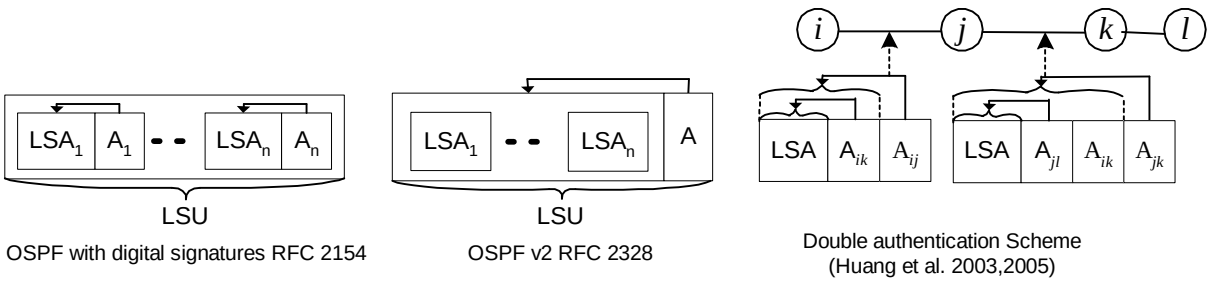


**Figure 4: Feature of different preventative schemes**