Mechanismen der zufallsbedingten Schlüsselvorverteilung in Sensornetzwerken

Nadine Rieß
Betreuerin: Corinna Schmitt
Seminar Sensorknoten: Betrieb, Netze und Anwendungen SS2010
Lehrstuhl Netzarchitekturen und Netzdienste, Lehrstuhl Betriebssysteme und Systemarchitektur
Fakultät für Informatik, Technische Universität München
Email: riess@in.tum.de

KURZFASSUNG

Diese Arbeit befasst sich mit der zufallsbedingten Vorverteilung von Schlüsseln in Sensornetzwerken. Aufgrund vielseitiger Einschränkungen bei Sensoren, wie zum Beispiel begrenzte Speicherressourcen oder geringe Rechenleistung, ist es nicht möglich, bewährte kryptographische Verfahren einzusetzen. Aus diesem Grund werden hier drei neue Mechanismen vorgestellt und hinsichtlich der Anforderungen an die Sensorknoten und die Sicherheit des Netzwerkes untersucht. Als Erstes wird das q-Verbundschlüssel-Schema näher betrachtet, womit klein angelegte Angriffe mit verhältnismäßig wenigen Knotenübernahmen effektiv reduziert werden können. Daraufhin folgt das Multipfad-Verstärkung-Schema, in dem die Sicherheit einer Kommunikationsverbindung zwischen zwei Knoten bei deren Etablierung erhöht wird. Zum Schluss wird auf das Zufalls-Schlüsselpaar-Schema eingegangen, welches bei kompromittierten Knoten die Sicherheit des restlichen Netzwerkes gewährleistet.

Schlüsselworte

Zufallsbedingte Schlüsselvorverteilung, Sensornetzwerk

1. EINLEITUNG

Sensornetzwerke werden heutzutage in vielen Bereichen eingesetzt, um verschiedenste Umgebungszustände zu erfassen oder zu überwachen. Dabei kann ein Netzwerk aus vielen tausend Sensorknoten bestehen, welche zur Ortung von Großflächenbränden, der Überwachung des Verkehrs in Realzeit, der Nachverfolgung von wild lebenden Tieren oder der Messung der Umweltverschmutzung dienen [1]. Auch der Einsatz im medizinischen Bereich zur Überwachung von lebensbedrohlichen Eigenschaften ist realisierbar. Sensoren erfreuen sich großer Beliebtheit aufgrund ihrer geringen Größe, der niedrigen Kosten und den weitreichenden Einsatzmöglichkeiten. Doch gerade bei sicherheitskritischen Anwendungen, wie Alarm- und Einbrucherkennungssystemen, ist es von enormer Wichtigkeit, dass die Sensoren zuverlässig arbeiten und nicht von außen manipuliert oder sogar außer Betrieb gesetzt werden.

Die Aufgabe besteht nun darin, die Sensoren vor dem Aufbau der Netzwerkverbindungen mit Kommunikationsschlüsseln auszustatten, so dass diese dann aufgrund verschlüsselter Kommunikationswege ein Netzwerk, mit gesicherten Verbindungen zwischen den Knoten, bilden. Es muss allerdings auch dafür gesorgt werden, dass Sensoren, die dem Netzwerk später beitreten möchten, die Möglichkeit haben, eine gesicherte Verbindung zu diesem aufzubauen. Dieser Aufbau des Netzwerkes inklusive der Aufnahmemöglichkeit später beitretender Sensoren wird als Bootstrapping-Problem bezeichnet [1]. Asymmetrische Kryptographieverfahren können aufgrund der begrenzten Hardwareausstattung der Sensoren, wie u. a. der geringen Speicherressourcen, nicht eingesetzt werden. Diese Einschränkungen und wichtige Sicherheitsaspekte, auf die im Hinblick auf sichere Kommunikation zu achten sind, werden in Kapitel 2 näher erläutert.

Das *Basisschema der zufallsbedingten Schlüsselvorverteilung* (basic random key predistribution scheme) von Eschenauer und Gligor [2] dient als Grundlage für die in dieser Arbeit diskutierten Mechanismen von H. Chan, A. Perrig und D. Song. Es geht davon aus, dass sich jeder Sensorknoten vor der Initialisierung des Netzwerkes m Schlüssel aus einer Menge von vorgegebenen Schlüsseln zufällig auswählt und diese in seinem Schlüsselring speichert. Mit Hilfe dieser Schlüssel können dann jeweils zwei benachbarte Knoten eine sichere Verbindung aufbauen, sofern sie einen gleichen Schlüssel aufgrund der vorherigen Zufallsverteilung besitzen und ihre Kommunikationsreichweiten ausreichen.
Das *q-Verbundschlüssel-Schema* (q-composite random key predistribution scheme) baut auf diesem Mechanismus auf und stellt die zusätzliche Anforderung, dass eine Kommunikation nur mit q anstatt mit einem einzigen gemeinsamen Schlüssel etabliert werden kann.
Das *Multipfad-Verstärkung-Schema* (multipath key reinforcement scheme) verbessert die Sicherheit beim Aufbau der gemeinsamen Verbindung zweier Knoten, da in diesem Fall mehrere disjunkte Teile eines Schlüssels über mehrere diskunkten Pfade verschickt und beim Endknoten wieder zum Schlüssel zusammengesetzt werden. So muss ein Angreifer mehr Knoten kompromittieren als bisher, damit eine Kommunikation zweier Knoten dechiffriert werden kann.
Zum Schluss wird auf das *Zufalls-Schlüsselpaar-Schema* (random-pairwise keys scheme) eingegangen, welches für jeweils zwei Knoten einen gemeinsamen Schlüssel vorsieht, den kein anderes Knotenpaar verwendet. Auch die gegenseitige Authentifizierung von Sensorknoten und die Implementierung einer Sperrliste der kompromittierten Knoten werden durch diesen Mechanismus ermöglicht.

Die Arbeit ist wie folgt aufgebaut: In Kapitel 2 wird zunächst auf die Restriktionen von Sensorknoten eingegangen und Kriterien zur Bewertung der Sicherheit vorgestellt. Danach wird eine Einführung in das Basisschema der zufallsbe-

dingten Schlüsselvorverteilung von Eschenauer und Gligor [2] in Kapitel 3 gegeben. Darauf aufbauend folgen das q-Verbundschlüssel-Schema in Kapitel 4, das Multipfad-Verstärkung-Schema in Kapitel 5 sowie das Zufalls-Schlüsselpaar-Schema in Kapitel 6, jeweils mit entsprechender Sicherheitsanalyse. In Kapitel 7 werden die einzelnen Mechanismen miteinander verglichen. Abschließend gibt es in Kapitel 8 eine Zusammenfassung der Ergebnisse.

2. RESTRIKTIONEN UND SICHERHEIT

Sensornetze unterliegen einigen Restriktionen. Die Sensorknoten sind hinsichtlich ihrer Rechenleistung und Speicherressourcen sehr beschränkt. Auch die Bandweite und Übertragungsleistung ist stark begrenzt, wodurch die Verlässlichkeit einer Datenübertragung gemindert wird. Bekannte asymmetrische Verschlüsselungsverfahren wie RSA [4] oder Schlüsselaustauschverfahren wie Diffie-Hellman [5] würden eine zu lange Berechnungszeit benötigen und sich wie eine Denial of Service (DOS) Attacke auswirken. Hinzu kommt, dass die Sensoren auch an öffentlichen oder sogar in feindlichen Gebieten platziert werden und sie einem Angreifer somit auch physikalisch ausgesetzt sind. Ein Sensorknoten hat auch vor der Initialisierung des Netzwerkes keinerlei Hinweise darauf, welcher und wieviele Knoten sich in seiner Nachbarschaft befinden werden. Viele Sensornetzwerke werden mit Basisstationen versehen, die als Vertrauensquelle gelten und zentrale Aufgaben übernehmen. Solche Basisstationen ziehen somit verstärkt das Interesse der Angreifer auf sich. Die nachfolgenden Mechanismen sollen ohne Basisstationen auskommen, um die Sicherheit zu erhöhen. All diese Punkte müssen bei der Entwicklung eines Mechanismus für die Schlüsselvorverteilung in Sensornetzwerken beachtet werden.

Da Sensorknoten hinsichtlich ihrer Sicherheit stark gefährdet sind, werden in dieser Arbeit besonders die folgenden Aspekte untersucht.

- Benötigte Speicherressourcen
- Widerstandsfähigkeit des Netzwerkes gegen kompromittierte Knoten
- Replikation von Sensorknoten
- Maximal unterstützbare Netzwerkgröße

Aufgrund des geringen Speicherplatzes der Sensoren muss darauf geachtet werden, die Datenmengen so gering wie möglich zu halten. Es können also nicht beliebig viele Daten abgespeichert werden, um damit bekannte Sicherheitsmechanismen zu realisieren. Wurden ein oder mehrere Knoten kompromittiert, dann soll ein Angreifer von den erhaltenen Daten keine bedeutenden Informationen über das Sensornetz
schließen können und der Rest des Netzwerkes widerstandsfähig gegen die feindliche Übernahme dieser Knoten bleiben. Des Weiteren muss darauf geachtet werden, dass das Sensornetz eine Resistenz gegenüber Duplikaten von Knoten aufweist. Es soll nicht möglich sein, Kopien der Sensorknoten anzufertigen, um diese für Attacken zu verwenden. Dazu können Sensoren Sperrlisten verwalten, welche es ermöglichen, kompromittierte Knoten abzuspeichern, um damit jede weitere Kommunikation mit ihnen zu unterbinden. Da unsichere Knoten gleichzeitig auch einen Teil des Netzwerkes unsicher machen, ist es interessant, die maximale Größe des unterstützbaren Netzwerkes zu kennen, bis zu der effektiver Schutz gewährleistet werden kann.

3. BASISSCHEMA DER ZUFALLSBEDINGTEN SCHLÜSSELVORVERTEILUNG

Die in dieser Arbeit beschriebenen Mechanismen bauen auf dem Basisschema der zufallsbedingten Schlüsselvorverteilung auf, welches nun kurz erläutert wird. Entwickelt wurde es von Eschenauer und Gligor [2] und lässt sich in drei verschiedene Phasen einteilen:

1. Initialisierungsphase
2. Konfigurationsphase
3. Pfadschlüssel-Aushandlungsphase

Zu Beginn der Initialisierungsphase wird ein *Schlüssel-Set S* von zufällig gewählten Schlüsseln vom gesamten möglichen Schlüsselraum extrahiert. Für jeden Sensorknoten werden nun wiederum m verschiedene Schlüssel vom Set S nach dem Zufallsprinzip ausgewählt und diese in dessen eigenen Schlüsselring abgelegt, welches in Abbildung 1 dargestellt ist. Die Anzahl der Schlüssel $|S|$ in der Schlüsselmenge wird dabei so gewählt, dass zwei Sensorknoten mit jeweils m gespeicherten Schlüsseln mindestens einen Schlüssel mit der Wahrscheinlichkeit p gemeinsam haben.

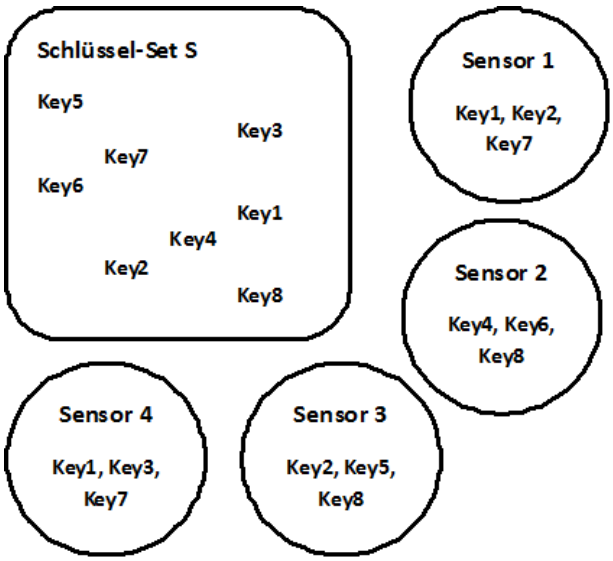

Abbildung 1: Schlüssel-Set S (Schlüsselringgröße m=3)

Ist die Initialisierung abgeschlossen, so werden in der darauf folgenden Konfigurationsphase die Sensorknoten aktiv und es erfolgt die Suche nach gemeinsamen Schlüsseln mit Nachbarknoten. Dazu wurde jedem Schlüssel in S ein kurzer *Identifikator* zugewiesen. Alle Sensorknoten senden nun einen Broadcast mit sämtlichen Identifikatoren. Falls ein Nachbarknoten einen gemeinsamen Identifikator, und damit einen

gemeinsamen Key, in seinem Schlüsselring entdeckt, so kann er diese Gemeinsamkeit durch ein *Challenge-Response-Protokoll* mit dem entsprechenden Nachbarknoten verifizieren. Ist dieser Schritt erfolgreich durchlaufen, so ist fortan der Schlüssel das gemeinsame Geheimnis zwischen den beiden Sensorknoten und sie können somit verschlüsselt kommunizieren. In der Abbildung 2 können beispielsweise Sensorknoten S3 und Sensorknoten S1 durch den Schlüssel K2 geheime Nachrichten austauschen.

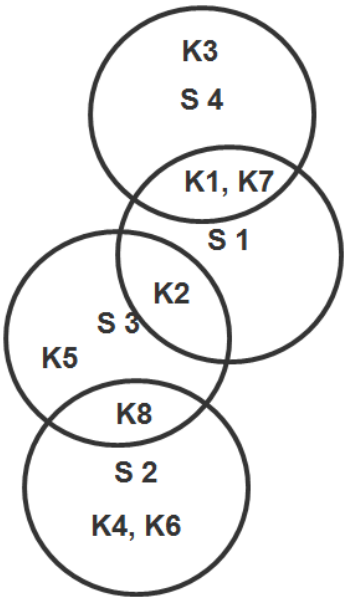

Abbildung 2: Kommunikationsverbindungen der Knoten

Nach der Konfigurationsphase ist ein Netzwerk aus miteinander verbundenen Knoten entstanden, welches als zusammenhängender Graph interpretiert werden kann. In der Aushandlungsphase ist es nun möglich, dass zwei Knoten, die bisher keinen gemeinsamen Schlüssel hatten, über einen entstandenen Pfad einen Schlüssel aushandeln. Falls der Graph also zusammenhängend ist, so kann ein Pfad vom Ausgangsknoten zu einem Nachbarknoten in Kommunikationsreichweite gefunden werden. Der Ausgangsknoten generiert dafür einen Pfadschlüssel und sendet ihn sicher über den Pfad an den Zielknoten [1]. Dadurch kann jeder Knoten zu allen Nachbarknoten direkte Verbindungen aufbauen.

4. Q-VERBUNDSCHLÜSSEL-SCHEMA

Das q-Verbundschlüssel-Schema ist dem Basisverfahren von Eschenauer und Gligor sehr ähnlich. Es unterscheidet sich lediglich darin, dass im q-Verbundschlüssel-Schema die Überlappung des Schlüsselringes der beiden Knoten von einem gemeinsamen Schlüssel auf q gemeinsame Schlüssel angehoben wird. Dies hat zur Folge, dass das Netzwerk widerstandsfähiger gegen Angriffe wird, da mehrere Schlüssel benötigt werden, um Verbindungen abzuhören. Somit wird es schwieriger für einen Angreifer, mit einer bereits erbeuteten Menge an Schlüsseln eine Verbindung zu belauschen. Um jedoch zu gewährleisten, dass zwei Sensorknoten sich q gemeinsame Schlüssel mit einer festgelegten Wahrscheinlichkeit p teilen, muss die Anzahl der Schlüssel in S gesenkt werden. Daraus folgt, dass auch der Angreifer weniger Knoten attackieren muss, um prozentual mehr Schlüssel aus S zu bekommen. Es ist eine Balance zwischen diesen konträren Faktoren zu finden, um die optimale Anzahl q und $|S|$ an Schlüsseln zu finden.

4.1 Funktionsweise des Algorithmus

Im Folgenden wird die genaue Vorgehensweise des Mechanismus dargestellt.

In der Initialisierungsphase wird eine Teilmenge an Schlüsseln aus dem gesamten Schlüsselraum gewählt. Von diesem werden wiederum Schlüssel extrahiert und im Schlüsselbund des Sensorknotens, welcher m Schlüssel umfasst, abgelegt.

In der Konfigurationsphase müssen nun wieder sämtliche Sensorknoten über die vorhandenen Schlüssel ihrer Nachbarknoten informiert werden. Dies könnte naiver Weise mit einem Broadcast der Schlüsselidentifikatoren an alle Knoten realisiert werden. Allerdings kann ein Angreifer die Verbindungen abhören und somit sämtliche ausgesendete Schlüsselsets eines Sensors aufzeichnen und diese Information dazu einsetzen, um gezielt Knoten anzugreifen und damit einen Großteil der Schlüssel in S in Erfahrung zu bringen. Eine sicherere, aber auch langsamere Methode stellen *Client-Puzzles* dar, wie beispielsweise das *Merkle-Puzzle* [6]. Jeder Knoten kann für jeden seiner m Schlüssel ein Client-Puzzle ausgeben. Der Sensor, der sich mit der richtigen Antwort rückmeldet, beweist, dass er den passenden Schlüssel besitzt.

Nachdem nun jeder Sensorknoten seine Nachbarknoten und deren Schlüsselmengen kennt, kann eine Verbindung initialisiert werden. Nur wenn die Anzahl der gemeinsamen Schlüssel zweier Knoten $q' \geq q$ ist, wird ein neuer Kommunikationsschlüssel K aus dem Hash aller gemeinsamen Schlüssel k_i generiert: $K = hash(k_1||k_2||\ldots||k_{q'})$. Gehasht wird nach einer kanonischen Ordnung, zum Beispiel darauf basierend, in welcher Ordnung die Schlüssel in der Schlüsselmenge S vorkommen [1].

Möchte nun ein neuer Sensorknoten dem Netzwerk beitreten, so durchläuft auch dieser die drei Phasen der Initialisierung, Konfiguration und Pfadschlüssel-Aushandlung. Zunächst wählt er zufällig m Schlüssel aus dem gesamten Schlüsselraum. Danach sendet er die entsprechenden Client-Puzzles und erhält von den Knoten mit dem passenden Schlüssel eine Antwort. Zum Schluss können wiederum Pfadschlüssel ausgehandelt werden.

4.2 Sicherheit

Das in diesem Abschnitt vorgestellte Schema ist nicht resistent gegen eine Replikation von Knoten, da die Anzahl der Verbindungen nicht beschränkt ist und es kein Limit gibt, wie oft ein Schlüssel genutzt werden kann. Das Schema kann allerdings eine *Sperrliste* von kompromittierten Knoten unterstützen, falls eine vertrauenswürdige Basisstation eingesetzt wird [1].

Die Widerstandsfähigkeit des Netzwerks gegen kompromittierte Knoten wird anhand der Gefahr, die von den erhaltenen Schlüsseln und den damit verbundenen Informationen des Knotens ausgeht, evaluiert. Man möchte also herausfinden, wie wahrscheinlich es ist, dass eine Verbindung zweier nicht kompromittierter Knoten entschlüsselt werden kann, falls ein Angreifer Sensorknoten des Netzes kompromittiert und versucht, aus den erhaltenen Daten die Schlüs-

selmenge S, und damit gleichzeitig das Set an Schlüsseln dieser Verbindung zu reproduzieren.
In Abbildung 3 wird gezeigt, dass bei einer niedrigeren Anzahl an kompromittierten Knoten die Widerstandsfähigkeit des Netzwerkes durch das q-Verbundschlüssel-Schema verbessert wird. Erhöht man q, so macht man es dem Angreifer schwerer an Teilinformationen mittels weniger Knotenübernahmen zu gelangen [1]. Im Gegensatz dazu weist dieser Mechanismus bei einem großen Netzwerk Schwächen auf. Hier wird es Angreifern erleichtert, an weitere Informationen zu gelangen, falls dieser bereits eine große Anzahl an Knoten kompromittiert hat. Dies ist allerdings ein wünschenswerter Kompromiss, weil Angriffe auf mengenmäßig wenige Knoten ("small-scale") viel schwieriger zu entdecken sind als groß angelegte Angriffe. Eine Attacke auf einen einzelnen Knoten kann im Gegensatz zu einer Attacke auf viele Knoten leicht als natürlicher Verbindungsabbruch getarnt werden.

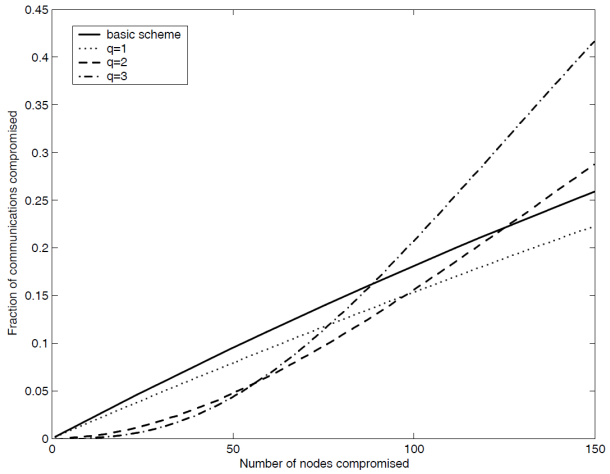

Abbildung 3: Wahrscheinlichkeit, dass eine Verbindung entschlüsselt werden kann, wenn daran nicht beteiligte Knoten kompromittiert wurden. (m=200, p=0,33) [1]

Eine feste Anzahl an kompromittierten Knoten bedeutet, dass ein bestimmter Anteil des Netzwerkes unsicher ist und die Mechanismen nicht für beliebig große Netzwerke verwendet werden können. Die maximal unterstützbare Größe eines Netzwerks ist so zu wählen, dass Angreifer bei einer festgelegten Anzahl von kompromittierten Knoten nur einen begrenzten Erfolg verbuchen können und nicht mehr über den Rest des Netzwerkes lernen, als sie über die Kommunikationschlüssel des kompromittierten Knotens selbst erfahren. Dadurch wird der Anreiz für einen Angriff gemindert, denn eine Attacke muss durch den Wert des einzelnen kompromittierten Knotens gerechtfertigt sein und nicht durch die Information, die die erhaltenen Schlüssel vom Rest des Netzwerkes preisgeben. Es existiert also ein Grenzwert der maximalen Menge an kompromittierten Informationen, ab der das Netzwerk als nicht mehr sicher gilt. Abbildung 4 stellt diesen Sachverhalt dar und berechnet den Grenzwert wie folgt. Sei x_m die Anzahl der kompromittierten Knoten. f_m ist der durch die x_m direkt kompromittierten Knoten und Verbindungen zusätzlich entstandene unsichere Teil des Netzwerkes. Der durchschnittliche Grad d eines Knotens bezeichnet die Anzahl der Verbindungen zu anderen Knoten. Der Angreifer hat somit $x_m d$ erwartete Verbindungen, in welche die kompromittierten Knoten verwickelt sind. Da es insgesamt $\frac{nd}{2}$ Verbindungen im Netzwerk gibt, ist die Forderung $(\frac{nd}{2} - x_m d) f_m \leq x_m d$.. Umgeformt ergibt sich die obere Schranke für die maximale Netzwerkgröße: $n \leq 2x_m \left(1 + \frac{1}{f_m}\right)$.

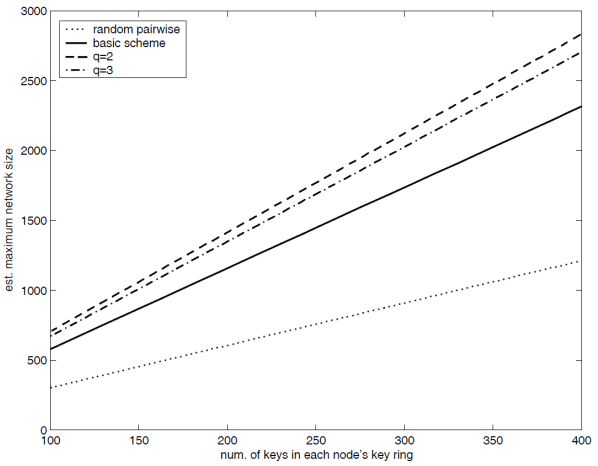

Abbildung 4: Maximale Netzwerkgröße (p=0,33, f_m=0,1) [1]

5. MULTIPFAD-VERSTÄRKUNG-SCHEMA

Dieses Kapitel behandelt den Mechanismus des Multipfad-Verstärkung-Schemas, dessen Grundidee von Anderson und Perrig stammt [3]. Das Ziel dieses Mechanismus ist es, die Sicherheit des Kommunikationsschlüssels zweier Knoten zu verbessern, indem dieser Schlüssel mittels mehrerer Pfade etabliert wird. Diese Herangehensweise führt allerdings dazu, dass der Netzwerkverkehr zunimmt.

5.1 Funktionsweise des Algorithmus

Beim Multipfad-Verstärkung-Schema findet die Initialisierungs- und Konfigurationsphase entsprechend dem Basisschema der zufallsbedingten Schlüsselvorverteilung statt und es wird angenommen, dass sichere Kommunikationsverbindungen mittels der vorhandenen Schlüssel aufgebaut wurden. Ein Schlüssel, der von zwei Sensorknoten genutzt wird, könnte damit noch in weiteren Schlüsselringen von anderen Knoten vorkommen und zu deren Kommunikation verwendet werden. Falls diese Knoten kompromittiert werden, so ist ebenfalls die Kommunikationssicherheit der beiden anderen Knoten, welche den gleichen Schlüssel nutzen, in Gefahr. Daher ist es sinnvoll, den gemeinsamen Schlüssel zweier Knoten nach der Konfigurationsphase durch einen neuen, zufällig gewählten auszutauschen, im Folgenden als *Schlüsselupdate* bezeichnet. Jedoch wäre es fahrlässig, den neuen Schlüssel über die direkte Verbindung, mit dem alten Schlüssel chiffriert, zu senden. Ist der alte Schlüssel bekannt, so kann der neue damit ebenfalls entschlüsselt werden.
Deshalb nutzt das Schlüsselupdate mehrere disjunkte Pfade von einem Knoten A zu einem Zielknoten B. Es werden nach der Konfigurationsphase genug Informationen bzgl. der bestehenden Routen im Netzwerk gesammelt. Somit sind alle

disjunkten Pfade von A zu B bekannt, die aus einer maximalen Anzahl an Hops bestehen. Die Abbildung 5 erklärt diesen Sachverhalt. Die Verbindung zwischen A und dem Sensorknoten S6 darf wegen der Disjunktheit lediglich einmal genutzt werden und der zweite Weg, markiert durch X, ist somit nicht zulässig. Angenommen, es wurden j disjunkte Pfade vom Sensorknoten A zu B während der Konfigurationsphase gefunden. Knoten A erzeugt nun j zufällige Werte, die der Länge eines gewöhnlichen Schlüssels entsprechen und sendet über jeden der j Pfade einen dieser Werte. B kann sich, sofern es alle j Werte erhalten hat, genauso wie A, aus diesen einen neuen Schlüssel $K = (k \otimes v_1 \otimes v_2 \otimes \ldots \otimes v_j)$ generieren, welcher von nun an als Kommunikationsschlüssel zwischen A und B genutzt wird [1].

Wenn lediglich Pfade über 2 Verbindungen untersucht werden, genannt *2-Hop-Multipfad-Verstärkung-Schema*, dann wird der Aufwand, alle Pfade zu finden, wesentlich reduziert. Zwei Knoten A und B, welche einen geheimen Schlüssel vereinbaren wollen, müssen lediglich eine Liste ihrer gemeinsamen Nachbarn erstellen. Desweiteren sind alle diese Pfade disjunkt, weshalb kein weiterer Aufwand betrieben werden muss, um die Disjunktheit zu garantieren.

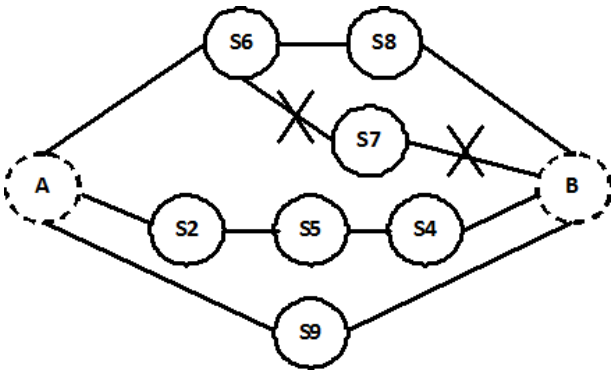

Abbildung 5: Disjunkte Pfade, max. Hoplänge=4

Auch in diesem Schema durchläuft ein neu hinzukommender Sensor die drei Phasen. Nach der zufälligen Auswahl der Schlüssel und dem Broadcast findet das Schlüsselupdate wie oben beschrieben statt.

5.2 Sicherheit

Die Sicherheit des neuen Kommunikationsschlüssels ist durch die j zufälligen Werte gegeben. Der Angreifer muss also sämtliche j Pfade abhören, um alle Werte zu bekommen und somit den neuen Schlüssel rekonstruieren zu können. Daraus folgt, je mehr Pfade zwischen zwei Knoten existieren, desto sicherer ist der neue Schlüssel. Allerdings steigt mit der Länge der Pfade die Wahrscheinlichkeit, dass ein Angreifer einen Knoten dieses Pfades kompromittiert und der Datenfluss mitgelesen wird. Der Pfad ist also unsicher, sobald ein Knoten dieses Pfades unsicher ist. Desweiteren benötigen lange Pfade einen enorm großen Kommunikationsaufwand aufgrund der Überprüfung auf Disjunktheit.

In Abbildung 6 kann man das Verhältnis von der Anzahl der kompromittierten Knoten zum Anteil der unsicheren Verbindungen ablesen. Das Basisschema und das q-Verbundschlüssel-Schema werden durch die Kombination mit dem 2-Hop-Multipfad-Verstärkung-Schema jeweils verbessert, wobei das Basisschema besser als das q-Verbundschlüssel-Schema für $q \geq 2$ ist. Dies liegt daran, dass das q-Verbundschlüssel-Schema nach dem gleichen Prinzip arbeitet wie das Multipfad-Schema, da es mehrere Schlüssel bzw. Pfade benötigt, um den neuen Schlüssel zu berechnen. Die Kompromisse die man beim Verbundschlüssel-Schema ($|S|$ wurde minimiert) und beim Multipfad (erhöhter Kommunikationsaufwand) eingegangen ist, wirken nun gleichzeitig gegen die Vorteile des Multipfad-Schemas und minimieren diese.

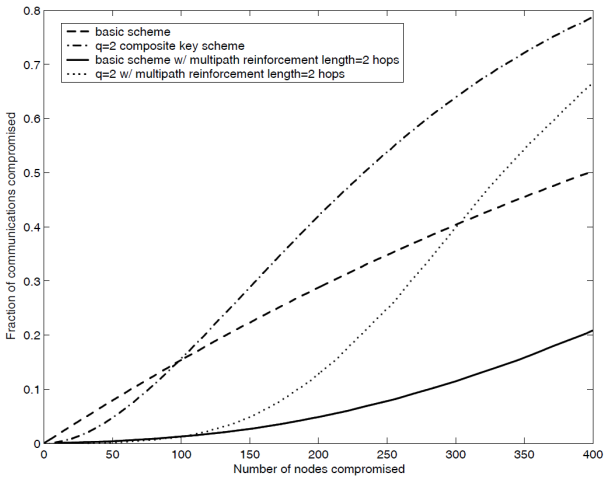

Abbildung 6: Resistenz gegen kompromittierte Knoten (m=200, p=0,33) [1]

In Abbildung 7 lässt sich ablesen, welche Anzahl an gespeicherten Schlüsseln im Knoten welche maximale Netzwerkgröße zulässt. Auch hier werden beide Mechanismen mit dem 2-Hop-Verfahren kombiniert und verglichen. Das Multipfad-Verfahren, angewandt auf das Basis-Verfahren, ermöglicht eine wesentlich größere Netzwerkgesamtgröße, hat aber beim q-Verbundschlüssel-Schema nur einen geringen Effekt.

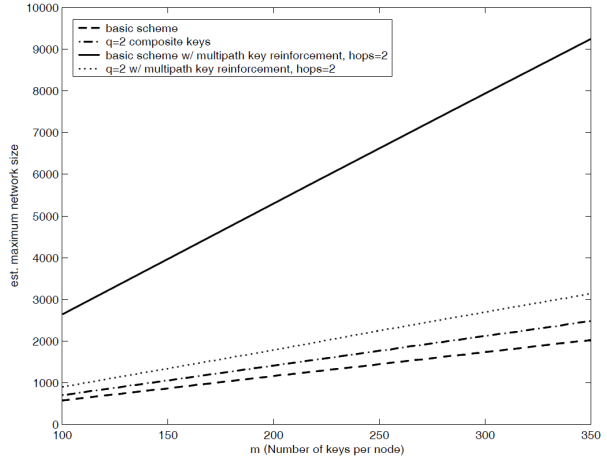

Abbildung 7: Maximale Netzwerkgröße (p=0,33) [1]

Der zusätzlichen Sicherheit durch den Multipfad-Mechanismus steht ein größerer Kommunikationsaufwand aufgrund der Suche nach disjunkten Pfaden und der Etablierung des neuen Schlüssels gegenüber. Ob dies ein guter Kompromiss ist, hängt von der spezifischen Anwendung und der Dichte des Sensornetzwerks selbst ab [1]. Mit dem Multipfad-Verfahren können aber auch Schlüssel für Knoten erzeugt werden, die nach der Konfigurationsphase keine Schlüssel miteinander teilen.

6. ZUFALLS-SCHLÜSSELPAAR-SCHEMA

In den bereits behandelten Mechanismen kann jeder Knoten bestätigen, dass sein Nachbarknoten bestimmte geheime Schlüssel besitzt und sich damit für eine Kommunikation qualifiziert. Allerdings ist kein Sensorknoten in der Lage den jeweils anderen zu authentifizieren, ihm ist also die Identität seines Kommunikationspartners nicht bekannt.
Beispielsweise teilt A mit B eine Menge K von geheimen Schlüsseln, womit sie ihre Kommunikation verschlüsseln. Da die Schlüssel auch mehrmals von S extrahiert und zugeteilt werden können, ist es möglich, dass ein Knoten C diese Menge K ebenfalls in seinem Schlüsselbund verwaltet. Knoten A kann also nicht sicher gehen, ob er mit B oder C kommuniziert. Die gegenseitige Verifikation von Knoten wird als *Knoten-zu-Knoten-Authentifizierung* (Node-to-Node-Authentification) bezeichnet und unterstützt viele Sicherheitsfunktionen.

6.1 Funktionsweise des Algorithmus

Angenommen ein Netzwerk besteht aus n Sensorknoten. Eine einfache Lösung des Schlüsselpaar-Schemas ist es, dass jeder Knoten *n-1* Kommunikationsschlüssel speichert, welche er mit jeweils einem anderen Knoten des Netzwerks teilt. Das Zufalls-Schlüsselpaar-Schema ist eine Modifikation davon, wobei aber nicht alle *n-1* Keys im Schlüsselbund abgespei- chert werden müssen, um einen zusammenhängenden Graph mit einer hohen Wahrscheinlichkeit zu erhalten. Wie oben bereits erwähnt wird in einem Sensornetzwerk mit der Wahrscheinlichkeit p eine Verbindung zwischen zwei Knoten aufgebaut. Somit muss ein Knoten nur np Schlüssel anstatt *n-1* Schlüssel in seinem Schlüsselring der Größe m abspei- chern. Dies ergibt die Formel $m = np$, was sich zu $n = \frac{m}{p}$ umformen lässt.
Die Nutzung von paarweise vergebenen Schlüsseln anstatt von zufällig gewählten Schlüsseln aus einer Menge S erlaubt Knoten-zu-Knoten Authentifizierung, falls jeder Sensor zum Schlüssel k die *Identität* (ID) des anderen Knotens abspeichert. Somit weiß jeder Sensorknoten anhand des genutzten Kommunikationsschlüssel mit welchem Knoten er kommuniziert.

In der Initialisierungsphase des Zufalls-Schlüsselpaar-Schemas werden zunächst n einzigartige Identitäten generiert. Falls das Netzwerk aktuell weniger als n Knoten besitzt, so können die verbleibenden Identitäten für später hinzukommende Knoten verwendet werden. Jede Knotenidentität wird nun mit m anderen IDs verbunden und die Schlüsselpaare für jeweils zwei Knoten werden generiert. Ein Schlüssel wird dann in beiden Knoten zusammen mit der ID des jeweils anderen Knotens gespeichert.
In der Konfigurationsphase findet nun ein Broadcast der eigenen Knoten-ID statt. Findet ein anderer Knoten diese ID in seinem eigenen Schlüsselbund, so initiiert er einen *kryptographischen Handshake* zwischen ihm und dem anderen Knoten, wodurch eine gegenseitige Authentifizierung stattfindet.

6.2 Erweiterung des Algorithmus

Da sich die Sensorknoten im Zufalls-Schlüsselpaar-Schema gegenseitig authentifizieren, kann der Mechanismus durch *Sperrlisten* für Knoten (node revocation list) erweitert werden. In diesen Sperrlisten werden Sensorknoten erfasst, die sich nicht konform verhalten und somit der Verdacht auf Manipulation naheliegt. Ist ein Knoten einmal notiert, so werden die anderen Knoten jegliche Kommunikationsanfragen von diesem zurückweisen. Normalerweise geschieht dies anhand von Basisstationen, welche die Listen abspeichern, auf Anfrage der Knoten ändern oder Informationen weitergeben. Aufgrund der hohen Latenzzeit zwischen den Knoten und der Basisstation ist dieses Verfahren extrem langsam, manipulierte Knoten müssen allerdings schnellstmöglich vom Netzwerk verbannt werden. Um diesem Nachteil zu entgehen, werden die Sperrlisten auf die Knoten verteilt.
Die Funktionsweise ist einer Wahl sehr ähnlich. Sensorknoten erhalten dabei eine Wahlstimme gegen einen Nachbarknoten, wenn sie mit ihm Kontakt aufgenommen haben. Erkennt nun ein Sensor eine verdächtige Handlung eines Nachbarn X, so wird der Sensor von seinem Stimmrecht Gebrauch machen und mittels Broadcast eine öffentliche Stimmabgabe gegen X versenden. Falls nun die Anzahl der Stimmen gegen X einen bestimmten Grenzwert übersteigt, so ist dieser Knoten als unsicher einzustufen und in die eigene Sperrliste aufzunehmen. Eine detailiertere Beschreibung kann in [1] nachgelesen werden.

6.3 Sicherheit

In diesem Verfahren authentifizieren sich die Sensorknoten gegenseitig und bestätigen somit ihre Identitäten. Es besteht die Möglichkeit, Knoten zu entlarven, die sich nicht konform verhalten und diese in eine Sperrliste aufzunehmen. Nicht konformes Verhalten können beispielsweise außergewöhnlich viele Broadcasts sein, die auf einen Denial of Service Angriff schließen lassen. Anstatt eine solche Sperrliste bei einer Basisstation zu verwalten, können die Knoten diese Aufgabe selbst übernehmen, was eine wesentliche Verbesserung der Reaktionszeit mit sich bringt. Somit lässt sich eine Kommunikation mit kompromittierten Knoten noch effektiver verhindern.
Des Weiteren können Kopien von Sensorknoten enttarnt werden, falls alle bereits initialisierten Knoten des Netzwerkes verwaltet werden und somit eine nochmalige Initialisierung der selben Identität auffallen würde. Andere Knoten werden dann eine Kontaktaufnahme zu diesem kopierten Sensor zurückweisen. Ein Knoten kann sich also nicht als ein anderer Knoten ausgeben und somit ist eine Replikation von Sensoren nicht möglich.
Die Widerstandsfähigkeit gegen kompromittierte Knoten ist optimal, denn durch die paarweise verteilten einzigartigen Keys kann ein Angreifer jeweils nur die Verbindungen entschlüsseln, in die der kompromittierte Knoten selbst verwickelt ist und bekommt keine weiteren Informationen über das Netzwerk.
Die maximal unterstützbare Größe des Netzwerks kann nicht nach dem Verfahren des q-Verbundschlüssel-Schema berechnet werden, da in diesem Fall ein kompromittierter Knoten keine weiteren Informationen über das Netzwerk preisgibt

[1]. Die maximale Netzwerkgröße kann also, wie in der Funktionsweise des Mechanismus bereits erwähnt, mit $n = \frac{m}{p}$ angegeben werden.

7. GEGENÜBERSTELLUNG DER ALGORITHMEN

Nun werden anhand der in Kapitel 2 genannten Bewertungskriterien die drei vorgestellten Mechanismen verglichen. Die Tabelle in Abbildung 8 zeigt hierfür das Basisschema von Eschenauer und Gligor (Basis) und das q-Verbundschlüssel-Schema für $q = 2$, jeweils mit und ohne der Anwendung des Multipfad-Verstärkung-Schemas, sowie das Zufalls-Schlüsselpaar-Schema. In der linken Spalte befinden sich die Bewertungskriterien. Die Zeichen + und - zeigen die Güte des Mechanismus im Gegensatz zu den anderen Verfahren an. Bei dem Kriterium der maximalen Netzwerkgröße wurde eine Rangfolge aufgestellt, wobei das Basisschema in Kombination mit dem Multipfad-Verstärkung-Schema deutlich größere Netzwerkkapazitäten zulässt als alle anderen Verfahren.

		Basis		2-Verbundschlüssel		Zufalls-Schlüsselpaar
		ohne Multipfad	mit Multipfad	ohne Multipfad	mit Multipfad	
Speicherbedarf		m Schlüssel m Identifikatoren		m Schlüssel m Identifikatoren		eigene KnotenID np Schlüssel np KnotenID's
Widerstands-fähigkeit bei Knotenübernahme (Anzahl Knoten)	wenige	--	++	-	++	+++
	viele	-	++	--	+	+++
Resistenz gegen Knoten-Replikation		Nein		Nein		Ja
Sperrliste		Ja (Basisstation)		Ja (Basisstation)		Ja
Max. Netzwerkgröße		4	1 ++	3	2	5

Abbildung 8: Vergleich aller Algorithmen

Aus der Tabelle ist ersichtlich, dass das Multipfad-Schema sowohl beim Basisschema als auch beim 2-Verbundschlüssel-Schema eine wesentliche Verbesserung der Wiederstandsfähigkeit bei Knotenübernahme erwirkt. Dennoch kann das Zufallsschlüsselpaar-Schema diesen Erfolg übertreffen. Letzteres bietet auch einen Schutz gegen Knoten-Replikation, da sich jeder Sensor gegenüber den anderen Sensoren authentifizieren muss. Eine Kopie eines Knotens, welche die Identität eines anderen für sich nutzt, kann somit identifiziert werden. Bei dem Kriterium der maximalen Netzwerkgröße wurde eine Rangfolge aufgestellt, wobei das Basis-Verfahren in Kombination mit dem Multipfad-Verfahren deutlich größere Netzwerkkapazitäten zulässt als alle anderen Verfahren. Das Zufalls-Schlüsselpaar-Schema ist nach [1] hinter dem Basisschema ohne Multipfad-Verstärkung-Schema einzuordnen.

8. ZUSAMMENFASSUNG

Sicherheit spielt in Sensornetzwerken eine große Rolle. Dabei wird nicht nur auf eine verschlüsselte Kommunikation zwischen den Sensoren Wert gelegt, sondern auch auf einen sicheren Eintritt von Sensoren, welche dem Netzwerk später beitreten. In dieser Arbeit wurden drei Mechanismen vorgestellt, die das Bootstrapping-Problem und damit verbundene Sicherheitsaspekte behandeln.
Das q-Verbundschlüssel-Schema ging dabei besonders auf den Verbindungsaufbau einer Kommunikation ein, was nur mit mehreren gemeinsamen Schlüsseln möglich ist. Dieses Schema verbesserte die Erkennung von "small-scale"-Attacken erheblich, führte allerdings auch zu einer größeren Verwundbarkeit bei großflächigen Angriffen.
Beim Multipfad-Verstärkung-Schema wurde für den Kommunikationsaufbau ein neuer Schlüssel generiert, welcher in Teilen über mehrere disjunkte Pfade zum Kommunikationspartner gesendet wird. Dies macht es für einen Angreifer schwerer, an den eigentlichen Schlüssel zu kommen, um die Kommunikation zwischen Knoten entschlüsseln zu können, jedoch ist dieses Verfahren mit einem erheblich größerem Kommunikationsaufwand im Netzwerk verbunden.
Zum Schluss ist das Zufalls-Schlüsselpaar-Schema, mit disjunkten Schlüsselpaaren für jeweils zwei Sensorknoten, untersucht worden. Dieser Mechanismus ist widerstandsfähig gegen kompromittierte Knoten, erkennt Replikationen von Knoten und ermöglicht eine Sperrliste.
Das Zufalls-Schlüsselpaar-Schema kann meiner Meinung nach aufgrund den Erkenntnissen aus Kapitel 7 als das beste Schema angesehen werden, sofern die Größe des auszubringenden Netzwerkes gering ist. Wird jedoch ein großes Netzwerk benötigt, so sollte das Basisverfahren in Kombination mit dem Multipfad-Verstärkung-Schema die erste Wahl sein.

9. LITERATUR

[1] H. Chan, A. Perrig, D. Song: *Random Key Predistribution Schemes for Sensor Networks*, IEEE Symposium on Security and Privacy, 2003.

[2] L. Eschenauer, V. D. Gligor: *A Key-Management Scheme for Distributed Sensor Networks*, Proceedings of the 9th ACM Conference on Computer and Communication Security, Seite 41-47, November 2002.

[3] R. Anderson, H. Chan, A. Perrig: *Key Infection: Smart Trust for Smart Dust*, Unpublished Manuscript, November 2001.

[4] R. L. Rivest, A. Shamir, L. Adleman: *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, 1978.

[5] W. Diffie, M. Hellman: *New directions in cryptography*, IEEE Transactions on information Theory, 1976.

[6] R. C. Merkle: *Secure communications over insecure channels*, Communications of the ACM, 1978.